

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号
特開2000-48076
(P2000-48076A)

(43)公開日 平成12年2月18日(2000.2.18)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 17/60		G 0 6 F 15/21	Z
9/06	5 5 0	9/06	5 5 0 Z
12/14	3 2 0	12/14	3 2 0 B
13/00	3 5 1	13/00	3 5 1 G
15/00	3 3 0	15/00	3 3 0 Z

審査請求 有 請求項の数19 O L (全 28 頁) 最終頁に続く

(21)出願番号 特願平10-213789

(22)出願日 平成10年7月29日(1998.7.29)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 中江 政行

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 100104916

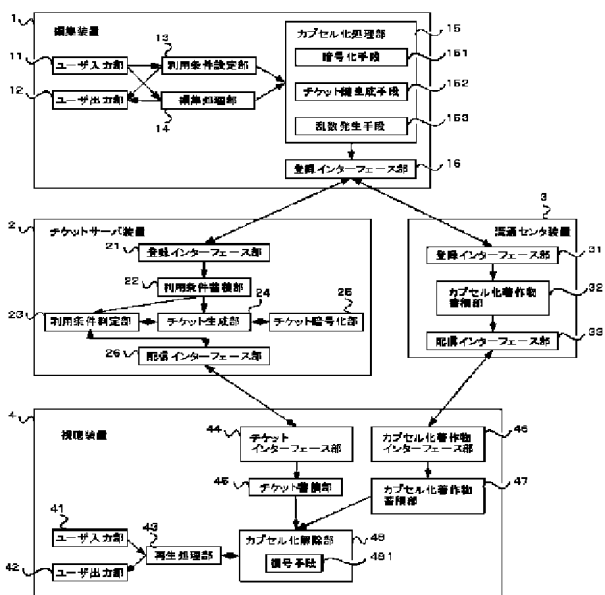
弁理士 古溝 聡 (外1名)

(54)【発明の名称】 デジタル著作物流通システム及び方法、デジタル著作物再生装置及び方法、並びに記録媒体

(57)【要約】

【課題】 デジタル著作物の流通に際して、詳細かつ柔軟な利用条件記述を行い、また、デジタル著作物の安全性を実現する。

【解決手段】 編集装置1は、利用法ごとの利用条件と、暗号化著作物データの復号鍵を利用法ごとに異なるチケット鍵により再暗号化した利用秘密情報とを、当該暗号化著作物データとともにカプセル化する。チケットサーバ装置2は、前記利用条件およびチケット鍵を管理し、利用者からの利用要求に対して利用法を許可した場合、前記チケット鍵を有したチケットを発行する。流通センタ装置3は、前記カプセル化著作物を管理し、利用者からの要求に応じてカプセル化著作物を配送する。視聴装置4は、流通センタ装置3からカプセル化著作物を取得し、その利用法に対するチケットをチケットサーバ装置2に要求する。視聴装置4は、当該チケットが取得された場合にのみ、前記カプセル化著作物に含まれる暗号化著作物データを復元し、再生する。



【特許請求の範囲】

【請求項1】配布すべき著作物データに利用条件を設定する利用条件設定手段と、

前記著作物データを所定の暗号鍵により暗号化する著作物暗号化手段と、

前記利用条件設定手段で設定された利用条件毎に、異なる複数のチケット暗号鍵及び対応する複数のチケット復号鍵を生成するチケット鍵生成手段と、

前記チケット鍵生成手段が利用条件毎に生成した複数のチケット暗号鍵で、前記所定の暗号鍵に対応する所定の復号鍵をそれぞれ暗号化する復号鍵暗号化手段と、

前記著作物データと、前記復号鍵暗号化手段で暗号化された利用条件毎の前記所定の復号鍵と、前記利用条件とをカプセル化したカプセル化著作物を生成するカプセル化手段と、

前記利用条件設定手段により設定された利用条件と、利用条件毎の暗号化に用いたチケット暗号鍵に対応するチケット復号鍵とを、それぞれ対応付けて蓄積する利用条件蓄積手段と、

外部からの前記著作物データの利用要求に応じて、該利用要求での利用条件に対応付けられて前記利用条件蓄積手段に蓄積されているチケット復号鍵を、前記利用要求の発信元の暗号鍵で暗号化するチケット復号鍵暗号化手段と、

前記チケット復号鍵暗号化手段で暗号化されたチケット復号鍵を、前記利用要求の発信元に配信するチケット配信手段とを備えることを特徴とするデジタル著作物流通システム。

【請求項2】前記カプセル化手段が生成したカプセル化著作物を蓄積するカプセル化著作物蓄積手段と、

前記カプセル化著作物蓄積手段に蓄積されたカプセル化著作物を配信するカプセル化著作物配信手段とをさらに備えることを特徴とする請求項1に記載のデジタル著作物流通システム。

【請求項3】前記所定の暗号鍵と、これに対応する前記復号鍵とは、共通暗号系を用いており、それぞれ同一の鍵であることを特徴とする請求項1または2に記載のデジタル著作物流通システム。

【請求項4】乱数を発生する乱数発生手段をさらに備え、

前記カプセル化著作物の暗号及び復号に使用する共通暗号系の鍵は、前記乱数発生手段が発生した乱数であることを特徴とする請求項3に記載のデジタル著作物流通システム。

【請求項5】前記複数のチケット暗号鍵と、これらのそれぞれに対応するチケット復号鍵とは、共通暗号系を用いており、それぞれ対応するもの同士が同一のチケット鍵で構成され、

前記チケット鍵生成手段は、利用条件毎に暗号と復号とに共通のチケット鍵を生成することを特徴とする請求項

1乃至4のいずれか1項に記載のデジタル著作物流通システム。

【請求項6】前記カプセル化手段によってカプセル化されたカプセル化著作物に含まれる著作物データから二次著作物データを生成する二次著作物データ生成手段を備え、前記配布すべき著作物データを、前記二次著作物データ生成手段によって生成された二次著作物データとし、

前記チケット鍵生成手段は、真のチケット暗号鍵及び対応する真のチケット復号鍵を生成する手段と、該真のチケット暗号鍵及び対応する真のチケット復号鍵並びに前記二次著作物データの基となる著作物データのチケット復号鍵から他の他のチケット復号鍵を生成する手段とを備え、

前記復号鍵暗号化手段は、前記二次著作物データの暗号鍵に対応する復号鍵をそれぞれ、前記真のチケット暗号鍵で暗号化し、

前記利用条件蓄積手段は、さらに前記他のチケット復号鍵を対応付けて蓄積することを特徴とする請求項1乃至5のいずれか1項に記載のデジタル著作物流通システム。

【請求項7】前記配布すべき著作物データに対して課金に関する処理を行わせるための課金モジュールを、前記利用条件設定手段によって設定された利用条件毎に生成する課金モジュール生成手段をさらに備え、

前記利用条件蓄積手段は、さらに課金モジュールに関する情報を各利用条件に対応付けて蓄積し、

前記カプセル化手段は、前記課金モジュール生成手段によって生成された利用条件毎の課金モジュールをさらにカプセル化したカプセル化著作物を生成することを特徴とする請求項1乃至5のいずれか1項に記載のデジタル著作物流通システム。

【請求項8】前記カプセル化手段がカプセル化したカプセル化著作物を取得するカプセル化著作物取得手段と、前記カプセル化著作物取得手段が取得した前記カプセル化著作物に含まれる所望の利用条件のチケット暗号鍵に対応するチケット復号鍵を取得するチケット復号鍵取得手段と、

前記チケット復号鍵取得手段が取得したチケット復号鍵で、前記カプセル化著作物に含まれる前記チケット暗号鍵で暗号化されている所定の復号鍵を復号する復号鍵復号手段と、

前記復号鍵復号手段が復号した所定の復号鍵で、前記カプセル化著作物に含まれる前記著作物データを復号する著作物復号手段と、

前記著作物復号手段で復号した著作物データを再生する再生手段とをさらに備えることを特徴とする請求項1乃至5のいずれか1項に記載のデジタル著作物流通システム。

【請求項9】前記配布すべき著作物データに対して課金

に関する処理を行わせるための課金モジュールを、前記利用条件設定手段によって設定された利用条件毎に生成する課金モジュール生成手段をさらに備え、
 前記利用条件蓄積手段は、さらに課金モジュールに関する情報を各利用条件に対応付けて蓄積し、
 前記カプセル化手段は、前記課金モジュール生成手段によって生成された利用条件毎の課金モジュールをさらにカプセル化したカプセル化著作物を生成し、
 前記カプセル化著作物取得手段が取得した前記カプセル化著作物に含まれる課金モジュールを抽出して蓄積する課金モジュール蓄積手段と、
 前記課金モジュール蓄積手段に蓄積されている課金モジュールのうちで、前記チケット鍵取得手段が取得したチケット復号鍵に対応する利用条件に応じたものに従って前記著作物データに対する課金処理を実行する課金処理手段とをさらに備えることを特徴とする請求項8に記載のデジタル著作物流通システム。

【請求項10】所定の暗号鍵により暗号化された著作物データと、前記著作物データの利用条件と、前記利用条件毎に異なるチケット暗号鍵で暗号化した前記所定の暗号鍵に対応する複数の復号鍵とをカプセル化したカプセル化著作物を取得するカプセル化著作物取得手段と、
 前記カプセル化著作物取得手段が取得した前記カプセル化著作物に含まれる所望の利用条件のチケット暗号鍵に対応するチケット復号鍵を取得するチケット復号鍵取得手段と、
 前記チケット復号鍵取得手段が取得したチケット復号鍵で、前記カプセル化著作物に含まれる前記チケット暗号鍵で暗号化されている所定の復号鍵を復号する復号鍵復号手段と、
 前記復号鍵復号手段が復号した所定の復号鍵で、前記カプセル化著作物に含まれる前記著作物データを復号する著作物復号手段と前記著作物復号手段で復号した著作物データを再生する再生手段とを備えることを特徴とするデジタル著作物再生装置。

【請求項11】前記カプセル化著作物取得手段が取得するカプセル化著作物は、さらに前記著作物データ毎の課金モジュールをカプセル化したものであり、
 前記チケット鍵取得手段は、さらに利用条件に応じた課金モジュールに関する情報を取得し、
 前記カプセル化著作物取得手段が取得した前記カプセル化著作物に含まれる課金モジュールを抽出して蓄積する課金モジュール蓄積手段と、
 前記課金モジュール蓄積手段に蓄積されている課金モジュールのうちで、前記チケット鍵取得手段が取得したチケット復号鍵に対応する利用条件に応じたものに従って前記著作物データに対する課金処理を実行する課金処理手段とをさらに備えることを特徴とする請求項10に記載のデジタル著作物再生装置。

【請求項12】配布すべき著作物データに利用条件を設

定する利用条件設定ステップと、
 前記著作物データを所定の暗号鍵により暗号化する著作物暗号化ステップと、
 前記利用条件設定ステップで設定された利用条件毎に、異なる複数のチケット暗号鍵及び対応する複数のチケット復号鍵を生成するチケット鍵生成ステップと、
 前記チケット鍵生成ステップで利用条件毎に生成した複数のチケット暗号鍵で、前記所定の暗号鍵に対応する所定の復号鍵をそれぞれ暗号化する復号鍵暗号化ステップと、
 前記著作物データと、前記復号鍵暗号化ステップで暗号化された利用条件毎の前記所定の復号鍵と、前記利用条件とをカプセル化するカプセル化ステップと、前記利用条件設定ステップで設定された利用条件と、利用条件毎の暗号化に用いたチケット暗号鍵に対応するチケット復号鍵とを、それぞれ対応付けて蓄積する利用条件蓄積ステップと、
 外部からの前記著作物データの利用要求に応じて、該利用要求での利用条件に対応付けられて蓄積されているチケット復号鍵を、前記利用要求の発信元の暗号鍵で暗号化するチケット復号鍵暗号化ステップと、
 前記チケット復号鍵暗号化ステップで暗号化されたチケット復号鍵を、前記利用要求の発信元に配信するチケット配信ステップとを含むことを特徴とするデジタル著作物流通方法。

【請求項13】前記カプセル化ステップでカプセル化されたカプセル化著作物に含まれる著作物データから二次著作物データを生成する二次著作物データ生成ステップをさらに含み、
 前記配布すべき著作物データを、前記二次著作物データ生成手段によって生成された二次著作物データとし、
 前記チケット鍵生成ステップは、真のチケット暗号鍵及び対応する真のチケット復号鍵を生成するステップと、
 該真のチケット暗号鍵及び対応する真のチケット復号鍵並びに前記二次著作物データの基となる著作物データのチケット復号鍵から他の他のチケット復号鍵を生成するステップとを含み、
 前記復号鍵暗号化ステップは、前記二次著作物データの暗号鍵に対応する復号鍵をそれぞれ、前記真のチケット暗号鍵で暗号化し、
 前記利用条件蓄積ステップは、さらに前記他のチケット復号鍵を対応付けて蓄積することを特徴とする請求項12に記載のデジタル著作物流通方法。

【請求項14】前記配布すべき著作物データに対して課金に関する処理を行わせるための課金モジュールを、前記利用条件設定手段によって設定された利用条件毎に生成する課金モジュール生成ステップをさらに含み、
 前記利用条件蓄積ステップは、さらに課金モジュールに関する情報を各利用条件に対応付けて蓄積し、
 前記カプセル化ステップは、前記課金モジュール生成手

段によって生成された利用条件毎の課金モジュールをさらにカプセル化したカプセル化著作物を生成することを特徴とする請求項12に記載のデジタル著作物流通方法。

【請求項15】所定の暗号鍵により暗号化された著作物データと、前記著作物の利用条件と、前記利用条件毎に異なるチケット暗号鍵で暗号化した前記所定の暗号鍵に対応する複数の復号鍵とをカプセル化したカプセル化著作物を取得するカプセル化著作物取得ステップと、取得した前記カプセル化著作物に含まれる所望の利用条件のチケット暗号鍵に対応するチケット復号鍵を取得するチケット復号鍵取得ステップと、前記チケット復号鍵取得ステップで取得したチケット復号鍵で、前記カプセル化著作物に含まれる前記チケット暗号鍵で暗号化されている所定の復号鍵を復号する復号鍵復号ステップと、前記復号鍵復号ステップで復号した所定の復号鍵で、前記カプセル化著作物に含まれる前記著作物データを復号する著作物復号ステップとを含むことを特徴とするデジタル著作物再生方法。

【請求項16】配布すべき著作物データに利用条件を設定する利用条件設定ステップと、前記著作物データを所定の暗号鍵により暗号化する著作物暗号化ステップと、前記利用条件設定ステップで設定された利用条件毎に、異なる複数のチケット暗号鍵及び対応する複数のチケット復号鍵を生成するチケット鍵生成ステップと、前記チケット鍵生成ステップで利用条件毎に生成した複数のチケット暗号鍵で、前記所定の暗号鍵に対応する所定の復号鍵をそれぞれ暗号化する復号鍵暗号化ステップと、前記著作物データと、前記復号鍵暗号化ステップで暗号化された利用条件毎の前記所定の復号鍵と、前記利用条件とをカプセル化するカプセル化ステップと、前記利用条件設定ステップで設定された利用条件と、利用条件毎の暗号化に用いたチケット暗号鍵に対応するチケット復号鍵とを、それぞれ対応付けて蓄積する利用条件蓄積ステップと、外部からの前記著作物データの利用要求に応じて、該利用要求での利用条件に対応付けられて蓄積されているチケット復号鍵を、前記利用要求の発信元の暗号鍵で暗号化するチケット復号鍵暗号化ステップと、前記チケット復号鍵暗号化ステップで暗号化されたチケット復号鍵を、前記利用要求の発信元に配信するチケット配信ステップとを実行するプログラムを記録することを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項17】前記カプセル化ステップでカプセル化されたカプセル化著作物に含まれる著作物データから二次著作物データを生成する二次著作物データ生成ステップをさらに含み、

前記配布すべき著作物データを、前記二次著作物データ生成手段によって生成された二次著作物データとし、前記チケット鍵生成ステップは、真のチケット暗号鍵及び対応する真のチケット復号鍵を生成するステップと、該真のチケット暗号鍵及び対応する真のチケット復号鍵並びに前記二次著作物データの基となる著作物データのチケット復号鍵から他の他のチケット復号鍵を生成するステップとを含み、

前記復号鍵暗号化ステップは、前記二次著作物データの暗号鍵に対応する復号鍵をそれぞれ、前記真のチケット暗号鍵で暗号化し、

前記利用条件蓄積ステップは、さらに前記他のチケット復号鍵を対応付けて蓄積することを特徴とする請求項16に記載のコンピュータ読み取り可能な記録媒体。

【請求項18】前記配布すべき著作物データに対して課金に関する処理を行わせるための課金モジュールを、前記利用条件設定ステップで設定された利用条件毎に生成する課金モジュール生成ステップをさらに含み、前記利用条件蓄積ステップは、さらに課金モジュールに関する情報を各利用条件に対応付けて蓄積し、前記カプセル化ステップは、前記課金モジュール生成手段によって生成された利用条件毎の課金モジュールをさらにカプセル化したカプセル化著作物を生成することを特徴とする請求項16に記載のコンピュータ読み取り可能な記録媒体。

【請求項19】所定の暗号鍵により暗号化された著作物データと、前記著作物の利用条件と、前記利用条件毎に異なるチケット暗号鍵で暗号化した前記所定の暗号鍵に対応する複数の復号鍵とをカプセル化したカプセル化著作物を取得するカプセル化著作物取得ステップと、取得した前記カプセル化著作物に含まれる所望の利用条件のチケット暗号鍵に対応するチケット復号鍵を取得するチケット復号鍵取得ステップと、前記チケット復号鍵取得ステップで取得したチケット復号鍵で、前記カプセル化著作物に含まれる前記チケット暗号鍵で暗号化されている所定の復号鍵を復号する復号鍵復号ステップと、前記復号鍵復号ステップで復号した所定の復号鍵で、前記カプセル化著作物に含まれる前記著作物データを復号する著作物復号ステップとを実行するプログラムを記録することを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタル著作物流通システム及び方法、デジタル著作物再生装置及び方法、並びにこれらのプログラムを記録したコンピュータ読み取り可能な記録媒体に関し、特にデジタル著作物の利用制御、二次著作物の利用制御、及びデジタル著作物に対する課金に関する。

【0002】

【従来の技術】従来、デジタル著作物流通システムは、ソフトウェアやマルチメディアコンテンツを暗号化し、利用者が販売者の示した利用規約に応じて相当額を、クレジットカードや銀行振込や電子現金などを介して、販売者に代金を収めるために用いられている。従来のデジタル著作物流通システムの一例が、特開平9-138827号公報に記載されている。

【0003】この公報に記載されたデジタル著作物流通システムは、流通センタ装置と利用者装置から構成されている。流通センタ装置では、利用者装置から要求された著作物について、適当な利用契約を結んだのち、利用者の公開鍵により当該著作物データを暗号化し、利用者装置へ送信する。

【0004】このとき、著作物データには利用条件が付加されており、前記利用者装置により解釈されて「参照のみ」や「編集可能」などの利用法制御が行なわれる。二次的著作物については、オリジナルデータと二次的著作に相当するデータおよび合成プログラムとがカプセル化され、オリジナルデータと同様に流通センタ装置を介して流通される。課金については、前記利用契約に記載された額の著作物の代金が課金される。

【0005】その他に、著作物は慣用暗号により暗号化し、所定の代金を支払ったときのみ、当該著作物の復号鍵を配信するような著作物流通システムも一般に良く知られている。一方、1988年USENIXカンファレンスプロシーディングス記載のKerberosシステムでは、認証情報Iが証明者Pが生成したものであることを、慣用暗号を用いて証明する方法が一般によく知られている。

【0006】この方法によると、1) Iおよびセッション鍵K_{p, v}を含んだ系列を信頼できる第三者が検証者V固有の鍵により暗号化したもの(チケット)とK_{c, s}を証明者Pに渡す。2) PはチケットをVに渡すとともに、3) IをK_{c, s}により暗号化したもの(認証子)をVに渡す。4) Vは、K_vを使ってチケットよりIおよびK_{p, v}を復号するとともに、K_{c, s}を使って認証子よりIを復号し、同じIが復号されたことを確認する。

【0007】同様の方法を、前記慣用暗号を利用した流通システムに適用すると、認証情報の代わりに著作物とし、セッション鍵の代わりに利用法に依存して決定される鍵とすると、慣用暗号により暗号化された著作物を配布した上で、利用時にチケット(著作物は含まれない)を配布することで、著作物の利用制御を行うことができる。

【0008】また、利用者の著作物に対する利用を細かく制限するようなデジタル著作物流通システムでは、著作物に予め利用不可能な利用法を列挙した禁止利用法リストを付加し、著作物視聴装置により、当該リストを解

釈して、各種利用法の実行可否を判断する。この種のデジタル著作物流通システムの一例が、特開平9-269916号公報に記載されている。

【0009】この公報に記載されたデジタル著作物流通システムは、編集装置と、流通サーバ装置と、視聴装置とを有し、編集装置で著作物データの編集と、禁止利用法リストの作成を行い、両者を一つのカプセル化著作物に同梱する。そして、流通サーバ装置を介して、視聴装置に流通される。視聴装置では、前記カプセル化著作物を開梱し、禁止利用法リストを基に、各利用法に対応するプロセス間メッセージを阻止するようなフックを、視聴装置が動作するオペレーティングシステムに施すことで、前記リストに記載された利用法を禁止する。

【0010】また、二次的著作物に対する著作権保護を可能とするようなデジタル著作物流通システムでは、二次的著作物が前段の著作物の暗号鍵とは異なる二次暗号鍵を生成し、当該二次暗号鍵により二次的著作物を暗号化して流通させる。このとき、各次暗号鍵は、著作権管理センタにより管理され、以上のような二次的著作が行われたことを把握する。この種のデジタル著作物流通システムの一例が、特開平8-272745号公報に記載されている。

【0011】この公報に記載されたデジタル著作物流通システムは、一次著作物が一次暗号鍵により暗号化され、当該一次著作物を利用した二次著作物の作成・配布に際して、二次暗号鍵を新たに生成し、当該二次暗号鍵により前記二次著作物を暗号化し、配布する。当該二次著作物には、前記一次著作物の原データと、当該二次著作物を作成するための加工手順とが、同梱されている。前記一次著作物の原データの復元には、前記一次暗号鍵を用い、前記二次著作物全体を復元には、前記二次暗号鍵を用いる。

【0012】著作物への課金に関して、利用度数を監視し、利用度数を基にした従量課金を行うことのできる方法が提案されている。このような著作物利用制御システムの一例が、特開平8-95777号公報記載されている。

【0013】この公報に記載された著作物利用制御システムは、著作物に対して所定の利用が行われたときにその利用度数の計数を行う。当該著作物には、課金情報が含まれており、各利用に関して、一定回数の無料利用ができるような設定の他、利用度数を基にした課金方法を設定できるようになっている。

【0014】

【発明が解決しようとする課題】しかしながら、上記従来例には、次のような問題点があった。

【0015】第1の問題点は、著作者や販売者の著作物の配布に関する意図が十分反映されない点にある。その理由は、利用者が受け取ったカプセル化著作物データに対して、ある一つの固定された利用法制御しか行えない

ためである。したがって、異なる利用法制御を行おうとした場合、前記利用条件をいくつか作成し、それぞれについてカプセル化を行う必要があるが、著作者や販売者の意図を反映するに十分とは言えない。

【0016】第2の問題点は、利用条件を著作物に同梱するのは危険である点にある。その理由は、視聴装置で、利用条件が著作物データと共に不揮発性メモリに保持されるが、この際、利用条件に不正な変更が加えられる可能性があるためである。

【0017】第3の問題点は、二次的著作物の利用について効率が悪い点にある。その理由は、前記特開平8-272725号公報に記載されているような方法では、二次的著作物の利用の際、まず当該著作物に含まれる原著物の復元を行い、さらに当該二次的著作物に追加されたデータを復元する必要がある。通常、画像や動画などの著作物は、そのサイズが膨大であり、前記のような複数回の復号処理を行う方法では、再生処理のスループットの大幅な低下を引き起こすためである。

【0018】第4の問題点は、流通させる著作物の多様性を保つことが困難な点にある。その理由は、課金方法がシステムにより予め定められていたり、利用度数など課金単位が固定的であったりすると、動画を用いた映画的作品（ペイ・パー・ビュー向き）や書籍的作品（売切向き）など、様々な形態をもった著作物を包括的に扱うことが困難なためである。

【0019】本発明の第1の目的は、デジタル著作物の流通に関し、著作者および販売者の意図を反映させるために、詳細かつ柔軟な利用条件記述を行う手段を提供することにある。

【0020】本発明の第2の目的は、デジタル著作物のより強固な安全性を実現することにある。

【0021】本発明の第3の目的は、二次的著作物の利用において、当該著作物に関係する任意の権原者の権利主張を可能にし、二次的著作物の再生処理時の、暗号化著作物データの復号によるスループット低下を抑制することにある。

【0022】本発明の第4の目的は、デジタル著作物に対する課金処理の柔軟性向上にある。

【0023】

【課題を解決するための手段】上記第1、第2の目的を達成するため、本発明の第1の観点にかかるデジタル著作物流通システムは、配布すべき著作物データに利用条件を設定する利用条件設定手段と、前記著作物データを所定の暗号鍵により暗号化する著作物暗号化手段と、前記利用条件設定手段で設定された利用条件毎に、異なる複数のチケット暗号鍵及び対応する複数のチケット復号鍵を生成するチケット鍵生成手段と、前記チケット鍵生成手段が利用条件毎に生成した複数のチケット暗号鍵で、前記所定の暗号鍵に対応する所定の復号鍵をそれぞれ暗号化する復号鍵暗号化手段と、前記著作物データ

と、前記復号鍵暗号化手段で暗号化された利用条件毎の前記所定の復号鍵と、前記利用条件とをカプセル化したカプセル化著作物を生成するカプセル化手段と、前記利用条件設定手段により設定された利用条件と、利用条件毎の暗号化に用いたチケット暗号鍵に対応するチケット復号鍵とを、それぞれ対応付けて蓄積する利用条件蓄積手段と、外部からの前記著作物データの利用要求に応じて、該利用要求での利用条件に対応付けられて前記利用条件蓄積手段に蓄積されているチケット復号鍵を、前記利用要求の発信元の暗号鍵で暗号化するチケット復号鍵暗号化手段と、前記チケット復号鍵暗号化手段で暗号化されたチケット復号鍵を、前記利用要求の発信元に配信するチケット配信手段とを備えることを特徴とする。

【0024】上記デジタル著作物流通システムでは、配信されるカプセル化著作物にはその著作物データの復号鍵が含まれていないため、著作物データを自由に配布することが可能となる。そして、著作物データを利用させる場合には、チケット配信手段からチケット復号鍵を配信するだけでよく、著作物の流通範囲の拡大と利用促進を望めるようになる。

【0025】また、利用条件設定手段によって著作物データの利用条件が設定され、その利用条件毎に異なるチケット鍵（暗号鍵及び復号鍵）が生成される。このため、著作者及び販売者の意図を反映させて、利用条件を設定し、著作物データを利用させることができる。

【0026】上記デジタル著作物流通システムは、前記カプセル化手段が生成したカプセル化著作物を蓄積するカプセル化著作物蓄積手段と、前記カプセル化著作物蓄積手段に蓄積されたカプセル化著作物を配信するカプセル化著作物配信手段とをさらに備えるものとしてもよい。

【0027】上記デジタル著作物流通システムにおいて、前記所定の暗号鍵と、これに対応する前記復号鍵とは、共通暗号系を用いて、それぞれ同一の鍵とすることができる。

【0028】上記デジタル著作物流通システムは、乱数を発生する乱数発生手段をさらに備えるものとしてすることができる。この場合、前記カプセル化著作物の暗号及び復号に使用する共通暗号系の鍵は、前記乱数発生手段が発生した乱数とすることができる。

【0029】また、上記デジタル著作物流通システムにおいて、前記複数のチケット暗号鍵と、これらのそれぞれに対応するチケット復号鍵とは、共通暗号系を用いて、それぞれ対応するもの同士が同一のチケット鍵で構成されたものとしてすることができる。この場合、前記チケット鍵生成手段は、利用条件毎に暗号と復号とに共通のチケット鍵を生成するものとしてすることができる。

【0030】さらに上記第3の目的を達成するため、上記デジタル著作物流通システムは、前記カプセル化手段によってカプセル化されたカプセル化著作物に含まれる

著作物データから二次著作物データを生成する二次著作物データ生成手段を備えるものとしてもよい。この場合、前記配布すべき著作物データを、前記二次著作物データ生成手段によって生成された二次著作物データとすることができる。そして、前記チケット鍵生成手段は、真のチケット暗号鍵及び対応する真のチケット復号鍵を生成する手段と、該真のチケット暗号鍵及び対応する真のチケット復号鍵並びに前記二次著作物データの基となる著作物データのチケット復号鍵から他の他のチケット復号鍵を生成する手段とを備え、前記復号鍵暗号化手段は、前記二次著作物データの暗号鍵に対応する復号鍵をそれぞれ、前記真のチケット暗号鍵で暗号化し、前記利用条件蓄積手段は、さらに前記他のチケット復号鍵を対応付けて蓄積するものとすることができる。

【0031】この場合、二次著作物データを一次著作物データと同様に流通させることができるので、著作活動の活性化が可能となる。また、二次著作物データの利用には真のチケット復号鍵が必要となるが、このためには、その基となる著作物データのチケット復号鍵と前記他のチケット復号鍵とが必要となるので、一次作者の権利保護を十分に図ることができる。

【0032】さらに上記第4の目的を達成するため、上記デジタル著作物流通システムは、前記配布すべき著作物データに対して課金に関する処理を行わせるための課金モジュールを、前記利用条件設定手段によって設定された利用条件毎に生成する課金モジュール生成手段をさらに備えるものとすることができる。この場合、前記利用条件蓄積手段は、さらに課金モジュールに関する情報を各利用条件に対応付けて蓄積し、前記カプセル化手段は、前記課金モジュール生成手段によって生成された利用条件毎の課金モジュールをさらにカプセル化したカプセル化著作物を生成することができる。

【0033】この場合、課金処理が課金モジュールで行われることとなり、しかも利用条件毎に生成が可能であるため、作者や販売者の意図、或いは著作物の性格などに従って、適切な課金方法を柔軟に選択することができる。

【0034】また、上記デジタル著作物流通システムは、前記カプセル化手段がカプセル化したカプセル化著作物を取得するカプセル化著作物取得手段と、前記カプセル化著作物取得手段が取得した前記カプセル化著作物に含まれる所望の利用条件のチケット暗号鍵に対応するチケット復号鍵を取得するチケット復号鍵取得手段と、前記チケット復号鍵取得手段が取得したチケット復号鍵で、前記カプセル化著作物に含まれる前記チケット暗号鍵で暗号化されている所定の復号鍵を復号する復号鍵復号手段と、前記復号鍵復号手段が復号した所定の復号鍵で、前記カプセル化著作物に含まれる前記著作物データを復号する著作物復号手段と、前記著作物復号手段で復号した著作物データを再生する再生手段とをさらに備え

るものとすることができる。

【0035】このような構成とした場合には、上記デジタル著作物流通システムは、前記配布すべき著作物データに対して課金に関する処理を行わせるための課金モジュールを、前記利用条件設定手段によって設定された利用条件毎に生成する課金モジュール生成手段をさらに備えるものとし、前記利用条件蓄積手段は、さらに課金モジュールに関する情報を各利用条件に対応付けて蓄積するものとすることができる。この場合、前記カプセル化手段は、前記課金モジュール生成手段によって生成された利用条件毎の課金モジュールをさらにカプセル化したカプセル化著作物を生成するものとなる。そして、上記デジタル著作物流通システムは、前記カプセル化著作物取得手段が取得した前記カプセル化著作物に含まれる課金モジュールを抽出して蓄積する課金モジュール蓄積手段と、前記課金モジュール蓄積手段に蓄積されている課金モジュールのうちで、前記チケット鍵取得手段が取得したチケット復号鍵に対応する利用条件に応じたものに従って前記著作物データに対する課金処理を実行する課金処理手段とをさらに備えるものとすることができる。

【0036】上記第1、第2の目的を達成するため、本発明の第2の観点にかかるデジタル著作物再生装置は、所定の暗号鍵により暗号化された著作物データと、前記著作物データの利用条件と、前記利用条件毎に異なるチケット暗号鍵で暗号化した前記所定の暗号鍵に対応する複数の復号鍵とをカプセル化したカプセル化著作物を取得するカプセル化著作物取得手段と、前記カプセル化著作物取得手段が取得した前記カプセル化著作物に含まれる所望の利用条件のチケット暗号鍵に対応するチケット復号鍵を取得するチケット復号鍵取得手段と、前記チケット復号鍵取得手段が取得したチケット復号鍵で、前記カプセル化著作物に含まれる前記チケット暗号鍵で暗号化されている所定の復号鍵を復号する復号鍵復号手段と、前記復号鍵復号手段が復号した所定の復号鍵で、前記カプセル化著作物に含まれる前記著作物データを復号する著作物復号手段と前記著作物復号手段で復号した著作物データを再生する再生手段とを備えることを特徴とする。

【0037】さらに上記第4の目的を達成するため、上記デジタル著作物再生装置において、前記カプセル化著作物取得手段が取得するカプセル化著作物は、さらに前記著作物データ毎の課金モジュールをカプセル化したものとし、前記チケット鍵取得手段は、さらに利用条件に応じた課金モジュールに関する情報を取得するものとする。この場合、上記デジタル著作物再生装置は、前記カプセル化著作物取得手段が取得した前記カプセル化著作物に含まれる課金モジュールを抽出して蓄積する課金モジュール蓄積手段と、前記課金モジュール蓄積手段に蓄積されている課金モジュールのうちで、前

記チケット鍵取得手段が取得したチケット復号鍵に対応する利用条件に応じたものに従って前記著作物データに対する課金処理を実行する課金処理手段とをさらに備えるものとするができる。

【0038】上記第1、第2の目的を達成するため、本発明の第3の観点にかかるデジタル著作物流通方法は、配布すべき著作物データに利用条件を設定する利用条件設定ステップと、前記著作物データを所定の暗号鍵により暗号化する著作物暗号化ステップと、前記利用条件設定ステップで設定された利用条件毎に、異なる複数のチケット暗号鍵及び対応する複数のチケット復号鍵を生成するチケット鍵生成ステップと、前記チケット鍵生成ステップで利用条件毎に生成した複数のチケット暗号鍵で、前記所定の暗号鍵に対応する所定の復号鍵をそれぞれ暗号化する復号鍵暗号化ステップと、前記著作物データと、前記復号鍵暗号化ステップで暗号化された利用条件毎の前記所定の復号鍵と、前記利用条件とをカプセル化するカプセル化ステップと、前記利用条件設定ステップで設定された利用条件と、利用条件毎の暗号化に用いたチケット暗号鍵に対応するチケット復号鍵とを、それぞれ対応付けて蓄積する利用条件蓄積ステップと、外部からの前記著作物データの利用要求に応じて、該利用要求での利用条件に対応付けられて蓄積されているチケット復号鍵を、前記利用要求の発信元の暗号鍵で暗号化するチケット復号鍵暗号化ステップと、前記チケット復号鍵暗号化ステップで暗号化されたチケット復号鍵を、前記利用要求の発信元に配信するチケット配信ステップとを含むことを特徴とする。

【0039】さらに上記第3の目的を達成するため、上記デジタル著作物流通方法は、前記カプセル化ステップでカプセル化されたカプセル化著作物に含まれる著作物データから二次著作物データを生成する二次著作物データ生成ステップをさらに含むものとするができる。この場合、前記配布すべき著作物データを、前記二次著作物データ生成手段によって生成された二次著作物データとしてもよい。そして、前記チケット鍵生成ステップは、真のチケット暗号鍵及び対応する真のチケット復号鍵を生成するステップと、該真のチケット暗号鍵及び対応する真のチケット復号鍵並びに前記二次著作物データの基となる著作物データのチケット復号鍵から他の他のチケット復号鍵を生成するステップとを含み、前記復号鍵暗号化ステップは、前記二次著作物データの暗号鍵に対応する復号鍵をそれぞれ、前記真のチケット暗号鍵で暗号化し、前記利用条件蓄積ステップは、さらに前記他のチケット復号鍵を対応付けて蓄積するものとするができる。

【0040】さらに上記第4の目的を達成するため、上記デジタル著作物流通方法は、前記配布すべき著作物データに対して課金に関する処理を行わせるための課金モジュールを、前記利用条件設定手段によって設定された

利用条件毎に生成する課金モジュール生成ステップをさらに含むものとしてもよい。この場合、前記利用条件蓄積ステップは、さらに課金モジュールに関する情報を各利用条件に対応付けて蓄積し、前記カプセル化ステップは、前記課金モジュール生成手段によって生成された利用条件毎の課金モジュールをさらにカプセル化したカプセル化著作物を生成するものとするができる。

【0041】上記第1、第2の目的と達成するため、本発明の第4の観点にかかるデジタル著作物再生方法は、所定の暗号鍵により暗号化された著作物データと、前記著作物の利用条件と、前記利用条件毎に異なるチケット暗号鍵で暗号化した前記所定の暗号鍵に対応する複数の復号鍵とをカプセル化したカプセル化著作物を取得するカプセル化著作物取得ステップと、取得した前記カプセル化著作物に含まれる所望の利用条件のチケット暗号鍵に対応するチケット復号鍵を取得するチケット復号鍵取得ステップと、前記チケット復号鍵取得ステップで取得したチケット復号鍵で、前記カプセル化著作物に含まれる前記チケット暗号鍵で暗号化されている所定の復号鍵を復号する復号鍵復号ステップと、前記復号鍵復号ステップで復号した所定の復号鍵で、前記カプセル化著作物に含まれる前記著作物データを復号する著作物復号ステップとを含むことを特徴とする。

【0042】上記第1、第2の目的を達成するため、本発明の第5の観点にかかるコンピュータ読み取り可能な記録媒体は、配布すべき著作物データに利用条件を設定する利用条件設定ステップと、前記著作物データを所定の暗号鍵により暗号化する著作物暗号化ステップと、前記利用条件設定ステップで設定された利用条件毎に、異なる複数のチケット暗号鍵及び対応する複数のチケット復号鍵を生成するチケット鍵生成ステップと、前記チケット鍵生成ステップで利用条件毎に生成した複数のチケット暗号鍵で、前記所定の暗号鍵に対応する所定の復号鍵をそれぞれ暗号化する復号鍵暗号化ステップと、前記著作物データと、前記復号鍵暗号化ステップで暗号化された利用条件毎の前記所定の復号鍵と、前記利用条件とをカプセル化するカプセル化ステップと、前記利用条件設定ステップで設定された利用条件と、利用条件毎の暗号化に用いたチケット暗号鍵に対応するチケット復号鍵とを、それぞれ対応付けて蓄積する利用条件蓄積ステップと、外部からの前記著作物データの利用要求に応じて、該利用要求での利用条件に対応付けられて蓄積されているチケット復号鍵を、前記利用要求の発信元の暗号鍵で暗号化するチケット復号鍵暗号化ステップと、前記チケット復号鍵暗号化ステップで暗号化されたチケット復号鍵を、前記利用要求の発信元に配信するチケット配信ステップとを実行するプログラムを記録することを特徴とする。

【0043】さらに上記第3の目的を達成するため、上記記録媒体は、前記カプセル化ステップでカプセル化さ

れたカプセル化著作物に含まれる著作物データから二次著作物データを生成する二次著作物データ生成ステップを実行するプログラムをさらに記録するものとして行うことができる。この場合、前記配布すべき著作物データを、前記二次著作物データ生成手段によって生成された二次著作物データとしてもよい。そして、前記チケット鍵生成ステップは、真のチケット暗号鍵及び対応する真のチケット復号鍵を生成するステップと、該真のチケット暗号鍵及び対応する真のチケット復号鍵並びに前記二次著作物データの基となる著作物データのチケット復号鍵から他の他のチケット復号鍵を生成するステップとを含み、前記復号鍵暗号化ステップは、前記二次著作物データの暗号鍵に対応する復号鍵をそれぞれ、前記真のチケット暗号鍵で暗号化し、前記利用条件蓄積ステップは、さらに前記他のチケット復号鍵を対応付けて蓄積するものとして行うことができる。

【0044】さらに上記第4の目的を達成するため、上記記録媒体は、前記配布すべき著作物データに対して課金に関する処理を行わせるための課金モジュールを、前記利用条件設定手段によって設定された利用条件毎に生成する課金モジュール生成ステップを実行するプログラムをさらに記録するものとしてもよい。この場合、前記利用条件蓄積ステップは、さらに課金モジュールに関する情報を各利用条件に対応付けて蓄積し、前記カプセル化ステップは、前記課金モジュール生成手段によって生成された利用条件毎の課金モジュールをさらにカプセル化したカプセル化著作物を生成するものとして行うことができる。

【0045】上記第1、第2の目的と達成するため、本発明の第6観点にかかる記録媒体は、所定の暗号鍵により暗号化された著作物データと、前記著作物の利用条件と、前記利用条件毎に異なるチケット暗号鍵で暗号化した前記所定の暗号鍵に対応する複数の復号鍵とをカプセル化したカプセル化著作物を取得するカプセル化著作物取得ステップと、取得した前記カプセル化著作物に含まれる所望の利用条件のチケット暗号鍵に対応するチケット復号鍵を取得するチケット復号鍵取得ステップと、前記チケット復号鍵取得ステップで取得したチケット復号鍵で、前記カプセル化著作物に含まれる前記チケット暗号鍵で暗号化されている所定の復号鍵を復号する復号鍵復号ステップと、前記復号鍵復号ステップで復号した所定の復号鍵で、前記カプセル化著作物に含まれる前記著作物データを復号する著作物復号ステップとを実行するプログラムを記録することを特徴とする。

【0046】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して詳細に説明する。

【0047】[第1の実施の形態]図1を参照すると、本発明の第1の実施の形態の著作物流通システムは、著作物データとその利用条件を編集し、カプセル化し、暗

号化する編集装置1と、チケットと利用条件を管理するチケットサーバ装置2と、暗号化された著作物を配布する流通センタ装置3と、利用者が著作物を利用する視聴装置4を含む。編集装置1は、著作者が保有し、チケットサーバ装置2および流通センタ装置3は、著作者もしくは販売代行者が保有・管理する。視聴装置4は、利用者が保有する。

【0048】編集装置1は、キーボード／マウスなどのユーザ入力部11と、モニタなどのユーザ出力部12と、利用条件設定部13と、編集処理部14と、カプセル化処理部15と、登録インターフェース部16を備えている。

【0049】利用条件設定部13は、編集処理部14で作成された著作物データに対する利用条件を、ユーザ入力部11とユーザ出力部12を介して著作者と対話的に作成する。

【0050】編集処理部14は、ユーザ入力部11からの入力に応じて著作物データを作成し、同時に作成された著作物データをユーザ出力部12に表示する。カプセル化処理部15は、暗号化手段151と、チケット鍵生成手段152と、乱数発生手段153とを備えており、乱数発生手段153より得られた一つの乱数Rと、チケット鍵生成手段152から得られた各チケット鍵を、暗号化手段151を用いて暗号化し、その結果から利用情報テーブルを作成するとともに、前記乱数Rと編集処理部14で作成された著作物データとを、暗号化手段151を用いて暗号化し、その結果と前記利用情報テーブルとを結合したカプセル化著作物データを生成する。

【0051】登録インターフェース部16は、チケットサーバ装置2へ前段までで生成した利用条件とチケット鍵を登録するための通信を行う。また、登録インターフェース部16は、流通センタ装置3へカプセル化著作物を蓄積するための通信を行う。

【0052】チケットサーバ装置2は、登録インターフェース部21と、利用条件蓄積部22と、利用条件判定部23と、チケット生成部24と、チケット暗号化部25と、配信インターフェース部26を備えている。

【0053】登録インターフェース部21は、編集装置1により作成された利用条件とチケット鍵の登録に伴う通信を行う。

【0054】利用条件蓄積部22は、登録インターフェース部21より得た利用条件およびチケット鍵を蓄積する。

【0055】利用条件判定部23は、配信インターフェース部26より得られた要求が利用条件に合致するかどうかを判定する。

【0056】チケット生成部24は、利用条件蓄積部22より利用条件とチケット鍵とから、チケットを生成する。

【0057】チケット暗号化部25は、利用条件判定部

23で合致すると判定された場合に適切なチケットを利用条件蓄積部22より取り出して利用者に応じて暗号化する。

【0058】配信インターフェース部26は、視聴装置4からの要求を受信するための通信を行い、チケット暗号化部25により生成された暗号化チケットを視聴装置4に送信するための通信を行う。

【0059】流通センタ装置3は、登録インターフェース部31と、カプセル化著作物蓄積部32と、配信インターフェース部33を備える。

【0060】登録インターフェース部31は、編集装置2で生成されたカプセル化著作物を受信するための通信を行なう。

【0061】カプセル化著作物蓄積部32は、登録インターフェース部31より受信されたカプセル化著作物を蓄積する。

【0062】配信インターフェース部33は、カプセル化著作物蓄積部32に蓄積された著作物のリストを作成し、視聴装置4へ送信するための通信と、視聴装置4からの要求を受信し、当該要求に応じたカプセル化著作物をカプセル化著作物蓄積部32より取り出し、視聴装置4へ送信するための通信とを行なう。

【0063】視聴装置4は、キーボード／マウスなどのユーザ入力部41と、モニタなどのユーザ出力部42と、再生処理部43と、チケットインターフェース部44と、チケット蓄積部45と、カプセル化著作物インターフェース部46と、カプセル化著作物蓄積部47と、カプセル化解除部48と、を備える。

【0064】再生処理部43は、カプセル化解除部48より得られた著作物データに記述されたプログラムを実行しながら、その入出力をユーザ入力部41とユーザ出力部42を介して行う。

【0065】チケットインターフェース部44は、再生処理部43を介してユーザから要求されたカプセル化著作物およびその利用法に応じて、チケットサーバ装置1よりチケットを受信するための通信を行う。

【0066】チケット蓄積部45は、チケットインターフェース部44より得たチケットを蓄積する。

【0067】カプセル化著作物インターフェース部46は、流通センタ装置3から著作物のリストを受信するための通信と、そのリストをユーザ出力部42に表示し、ユーザ入力部41により所望の著作物をユーザに選択してもらい、その結果に応じて流通センタ装置3から当該著作物を受信するための通信とを行う。

【0068】カプセル化著作物蓄積部47は、カプセル化著作物インターフェース部46より得られたカプセル化著作物を蓄積する。

【0069】カプセル化解除部48は、復号手段481を備えており、再生処理部43を介してユーザから要求されたカプセル化著作物を、カプセル化著作物蓄積部4

7より取得し、チケット蓄積部45より当該カプセル化著作物のチケットを取得し、当該カプセル化著作物および当該チケットから、復号手段481を用いて、著作物データを復元する。

【0070】なお、図1の著作物流通システムにおいて、編集装置1とチケットサーバ装置2、編集装置1と流通センタ装置3、チケットサーバ装置2と視聴装置4、流通センタ装置3と視聴装置4は、それぞれ互いにインターネットなどのネットワークを介して接続される。

【0071】以下、本実施の形態の動作について説明する。

【0072】まず、本実施の形態の動作全体の流れについて、図2を参照して説明する。著作者は、編集装置1を用いて著作物データの編集して流通センタ装置3に登録し、また、編集装置1を用いて利用条件の設定してチケットサーバ装置2に登録する（ステップA）。

【0073】次に、利用者は、流通センタ装置3から所望の著作物を取得し、視聴装置4に蓄積する（ステップB）。さらに、利用者は、その著作物について利用要求を行い、当該著作物のチケットをチケットサーバ装置2から取得して視聴装置4に蓄積する（ステップC）。そして、その利用者は、視聴装置4で当該著作物を利用する（ステップD）。

【0074】次に、図2のステップAの処理について、図3を参照して詳細に説明する。編集装置1で、著作者は著作物データを作成する。編集処理部14は一般的なマルチメディアオーサリングソフトウェアと同等の機能を備えており、対話的に著作物を作成することができる（ステップA1）。

【0075】そして当該著作物を流通させようとした時に、著作者は当該著作物に対する利用条件を設定する。この操作は、利用条件設定部13で制御され、図6のようなダイアログをユーザ出力部12を介して表示し、著作者はユーザ入力部11を操作して、図7のような手順で、利用法ごとの条件を設定していく（ステップA2）。

【0076】次に、カプセル化処理部15で、前段までで作成された著作物データと利用条件とからカプセル化著作物を生成する。

【0077】まず、暗号化手段151で、前記著作物データを乱数発生手段153より得た乱数Rにより暗号化する（ステップA3）。この際、共通鍵暗号を用いれば、暗号化および復号の処理にかかる時間を短くできる。

【0078】また、利用条件が設定された利用法uごとに、乱数発生手段153より乱数Ruを得ながら、チケット鍵生成部152によりRuを鍵として、前記著作物データ暗号鍵Rを暗号化手段151を用いて暗号化し、利用秘密情報E[Ru]（R）を得ていく（ステップA

4)。当該手順を示した模式図を図8に示す。ここで、式E[K](D)はデータDを鍵Kで共通鍵暗号化した結果を表し、以下同様の表記を用いる。

【0079】そして、前記利用条件と前記利用秘密情報から、図9に示すような利用法と利用秘密情報の組から成る表を作成する。これを利用秘密情報テーブルと呼ぶ。そして、前記利用秘密情報テーブルと前記暗号化著作物データと、著作者の氏名などで代表される著作者IDや著作物の名称である著作物IDやチケット発行元などの著作物情報とを連結して、図10に示したような構造をもつカプセル化著作物を生成する(ステップA5)。

【0080】前記利用条件は、図11に示すようなアクセス制御言語による形式的記述に変換される(ステップA6)。アクセス制御言語は、著作物を構成するオブジェクトごとに、可能な利用法が宣言され、利用法ごとに利用条件が宣言される形になっており、前記チケット鍵Ruは、利用法uに対する宣言中に埋め込まれる。すなわちオブジェクトを特定するIDを示し、次に利用法を表す文字列が示され、各種利用条件を表した条件語と各条件語へのパラメータを列挙し、次にチケット鍵を示す。ここでオブジェクトは、画像/テキストなどの基本的な構成要素を指す。

【0081】この場合、「モノクロ表示による閲覧」や「フルカラー表示による閲覧」などといったように、利用法をより詳細化して設定する場合には、例えば「モノクロ表示用オブジェクト」や「フルカラー表示用オブジェクト」などを用意し、視聴装置4で、特定機能を利用する場合に、それに応じたオブジェクトに対してチケットの発行を要求すればよい。また、特定機能とその対象となるオブジェクトの関係は、編集装置14での編集作業時に指定し、カプセル化著作物に当該情報を同梱すればよい。

【0082】基本的な構成要素の組み合わせや著作物全体といったように、オブジェクトに木構造を設ける場合について、利用条件を付す場合、上位のオブジェクトに属する下位のオブジェクト全てに共通した利用条件として宣言することもできる。まず、上位のオブジェクトを特定するIDを示し、次にその直接の子にあたるオブジェクトを示すIDを列挙し、次に前記同様、利用法を表す文字列が示され、条件語とそのパラメータの組を列挙する。ただし、最下位オブジェクトにおけるチケット鍵の宣言は、上位オブジェクトに対しては不用である。

【0083】例を示すと、構成要素1〜7をもつ著作物があって、その構成要素間の構造が図12(a)に示した形になっているとする。このとき、利用条件記述は、例えば図12(b)のようになる。

【0084】このような形の利用条件記述がチケットサーバ装置2で解釈される際には、各オブジェクトの利用条件は、先祖にあたるオブジェクトで宣言された利用条

件を継承する。ただし、上位のオブジェクトにおいてある条件が示され、同条件が、その子孫にあたるオブジェクトでも示されているとき、子孫にあたるオブジェクトの条件が優先される。

【0085】例えば、前記の例を用いると、(1)著作物全体に対して「表示可能な解像度が640×480以下」、(2)構成要素3に対して「構成要素1個当りの代金が10円」、(3)構成要素6に対して「代金が50円」とあった場合、構成要素6の代金は50円であり、表示可能解像度は640×480以下となる。一方、(4)構成要素7に対して「表示可能解像度が800×600以下」とあった場合、(1)および(2)および(4)より、構成要素7の代金は10円であり、表示可能解像度は800×600以下となる。

【0086】以上のようにして生成された利用条件記述は、登録インターフェース部16を通して、チケットサーバ装置2に登録される(ステップA7)。

【0087】そして、前記カプセル化著作物は、登録インターフェース部16を通して、流通センタ装置3に登録される(ステップA8)。

【0088】次に、図2のステップBの処理について、図4を参照して詳細に説明する。視聴装置4で、利用者はまず流通センタ装置3にアクセスし、著作物のカタログを得る(ステップB1)。このとき、例えば図13のようなインデックス画面がユーザ出力42を介して表示される。

【0089】利用者は、当該インデックス画面に表示された任意のリンクを辿り、希望の著作物を選択する(ステップB2)。当該要求を受けた流通センタ装置3では、カプセル化著作物蓄積部32より当該要求に応じて適切なカプセル化著作物を取得し、配信インターフェース部33を介して送信する。

【0090】視聴装置4では、当該カプセル化著作物を、カプセル化著作物インターフェース部46を介して受け取ったのち、カプセル化著作物蓄積部47に蓄積する(ステップB3)。

【0091】次に、図2のステップCの処理について、図5を参照して詳細に説明する。まず、利用者は、ステップB3でカプセル化著作物蓄積部47に蓄積した当該カプセル化著作物について、任意の利用法により利用要求を行う(ステップC1)。

【0092】前段で蓄積されたカプセル化著作物について、再生処理部43は利用法uについての処理を行なうため、まずカプセル化解除部48によって、当該カプセル化著作物に含まれる前記著作物情報と、前記利用秘密情報テーブルと、前記暗号化著作物データとに分割する。この分割後、カプセル化解除部48は、まず必要なチケットを既に取得済みかどうかを調べ、取得済みであれば、当該チケットを用いて後段の暗号化著作物データの復号を行なう。一方、未取得であった場合は、前記著

作物情報中のチケット発行元を参照して、対象となるチケットサーバ装置2を定め、チケットインターフェース部44を介して、当該チケットサーバ装置2に利用法uに対するチケットを要求する(ステップC2)。

【0093】チケットの要求には、「著作者ID」、「著作物ID」、「要求元利用者ID」、「要求する利用法」などの、利用対象である著作物と利用法を特定する情報と、「要求年月日」などの後に当該チケットの取引を証明するに十分な情報と、視聴装置4のユーザ表示部42の解像度や色数の上限などの表示性能およびユーザからの指示などから決定される利用時の条件が含まれる。

【0094】当該要求を受けたチケットサーバ装置2は、利用条件蓄積部22に蓄積された中から当該要求の対象となる著作物の利用条件を参照する(ステップC3)。

【0095】そして、当該利用条件を利用条件判定部23により解釈し、当該要求に対して前記利用法uのチケットを発行してよいかどうかを判定する(ステップC4)。判定項目としては、例えば「チケットを発行してよい利用者IDのリスト」があり、この場合前記要求に記載された利用者IDが前記リストに含まれれば当該チケットの発行を許可し、そうでなければ許可しない。不許可と判定された場合は、その旨を視聴装置4に通知し(ステップC5')、視聴装置4では当該チケットの発行が不許可になった旨をユーザ出力部42を介してユーザに知らせる(ステップC6')。この際、利用法uによる利用を行うことはできない。

【0096】前段で、発行してよいと判定された場合、チケット生成部24では、前記利用条件の前記利用法uについての条件が記述されたブロックを参照し、適切なチケット鍵を取得する。当該チケット鍵と、要求に記載された「利用者ID」、「利用法」などの前記要求に合致することを証明するに十分な情報を連結して、前記要求に対するチケットを生成する(ステップC5)。例えば、図14に示すように、「著作物ID」・「利用者ID」・「チケットシリアル番号」・「チケット鍵」・「許可された利用法」・「発行年月日」・「有効期限」を記載する。

【0097】当該チケットは、チケット暗号化部25により、前記利用者側の視聴装置4でのみ復号できるように、暗号化され、配信インターフェース部26により、前記視聴装置4に送信される(ステップC6)。この際、公開鍵暗号を用いることが望ましいが、Diffie-Hellman鍵共有プロトコルなどを用いて要求ごとに異なるセッション鍵を生成し、共通鍵暗号により暗号化してもよい。

【0098】視聴装置4では、当該チケットをチケットインターフェース部44により受信し、利用者の秘密鍵や前記セッション鍵などを用いて復号化し、チケット蓄

積部45に蓄積する(ステップC7)。

【0099】カプセル化解除部48は、前記利用法uに対するチケットと、前記アクセス制御テーブル中の閲覧ブロックを参照して(ステップC8)、それぞれから前記チケット鍵Ruと前記利用秘密情報E[Ru](R)を取り出し(ステップC9)、復号手段481を用いて、前記著作物復号鍵Rを復元する(ステップC10)。

【0100】そして、当該復号鍵Rと前記暗号化著作物データから、再び復号手段481を用いて著作物データを復元する。(ステップC11)。

【0101】次に、図2のステップDの処理について、詳細に説明する。再生処理部43は一時的な揮発性メモリを備えており、前段で復元された著作物データを当該揮発性メモリに保持する。そして、著作物データの内容を実行し、ユーザ入力部41とユーザ出力部42とを介して利用者と著作物との対話を処理する。

【0102】以上説明したように、本実施の形態では、著作物が暗号化され、上記利用秘密情報と共にカプセル化され、インターネットなどのネットワーク上で流通される。利用秘密情報は、暗号化された著作物データの復号鍵そのものではなく、復号鍵を得るには別途上記チケットを入手する必要がある。したがって、カプセル化された著作物は複製自由であり、上記流通センタ装置3を必ずしも経ずに、利用者間で譲渡しあうことができるため、著作物の流通速度の向上と、流通範囲の拡大につながる。また、利用法ごとにチケットが発行されるため、チケット1枚あたりの価格を低く抑えることができ、著作物の利用推進につながる。

【0103】[第2の実施の形態]図15を参照すると、本発明の第2の実施の形態の著作物流通システムは、図1に示された第1の実施の形態のものに加え、第1の視聴装置5を有する点で異なる。そして、編集装置7について、第1の実施の形態における編集装置1のカプセル化処理部15の構成に加え、鍵分割手段654を有する点で異なる。また、第2の視聴装置7について、第1の実施の形態における視聴装置4のカプセル化解除部の構成に加え、鍵統合手段782を有する点で異なる。

【0104】第1の視聴装置5は、図1に示された第1の実施の形態における視聴装置4と同様の構成であるが、ユーザ入力部41の指示により、カプセル化解除部48で復元された著作物データを編集装置6の編集処理部14に受け渡すことができる点で異なる。

【0105】鍵分割手段654は、カプセル化処理部15で、第1の視聴装置4により入手した第1のカプセル化著作物に対し、編集処理部14により再編集を加えた著作物データについて、第2のカプセル化著作物を作成する際に、第1のカプセル化著作物に対する第1のチケット鍵と乱数発生手段153から得た真のチケット鍵と

から、第2のカプセル化著作物に対する第2のチケット鍵を生成する。

【0106】鍵統合手段782は、第2のカプセル化著作物を利用するために、第1のチケット鍵および第2のチケット鍵とから、真のチケット鍵を復元する。

【0107】なお、図2の著作物流通システムでは、第1の視聴装置5と編集装置6とが、インターネットなどのネットワークを介して接続される。また、第1の視聴装置5及び第2の視聴装置7は、いずれもインターネットなどのネットワークを介してチケットサーバ装置2及び流通センタ装置3とそれぞれ接続される。

【0108】以下、本実施の形態の動作について、説明する。

【0109】まず、本実施の形態の動作全体の概略について、図16を参照して説明する。一次著作権者は、第1の実施の形態と同様にして、第1のカプセル化著作物を作成する(ステップA)。

【0110】二次著作権者は、第1の視聴装置5で、第1の実施の形態で利用者がしたのと同様に、前記第1の著作物を取得する(ステップB)。そして、二次著作権者は、再編集を要求し、その再編集要求を受けた第1の視聴装置5は、第1の実施の形態における視聴装置4と同様にチケットサーバ装置2に対して再編集チケットを要求する。そして、当該チケット要求を受けたチケットサーバ装置2では、再編集に対する利用条件判定を行い、当該条件が満たされれば、再編集チケットを第1の視聴装置5に送信する、これにより二次著作権者は、再編集チケットを取得する(ステップC)。さらに、編集装置6を用いて著作物データの編集して流通センタ装置3に登録し、また、編集装置6を用いて利用条件の設定してチケットサーバ装置2に登録する(ステップA1)。

【0111】次に、利用者は、第2の視聴装置7で、前記第2のカプセル化著作物を取得する(ステップB2)。さらに、利用者は、その第2のカプセル化著作物著作物について利用要求を行い、当該著作物のチケットをチケットサーバ装置2から取得して視聴装置4に蓄積する(ステップC)。そして、再生処理部43では当該著作物データを本発明の第1の実施の形態と同様の方法で再生する(ステップD)。

【0112】次に、図16のステップA'の処理について、図17を参照して詳細に説明する。当該再編集チケットを受信した第1の視聴装置5は、第1の実施の形態における視聴装置4と同様にして、再編集チケットを用いて第1の著作物データを復元し、編集装置6に渡す。その後、編集装置5における編集処理部14により、二次著作権者は当該著作物データを再編集し、第2の著作物データを作成する(ステップA'1)。

【0113】二次著作権者は、第2の著作物データに対して、利用条件設定部13で、第1の実施の形態における利用条件設定と同様の操作を行った後(ステップA'

2)、編集装置5は、暗号化手段151と乱数発生手段153を用いて、第2の著作物データを暗号化する(ステップA'3)。

【0114】その後、編集装置5は、条件が設定された各利用法Uについて、前記第1のカプセル化著作物に対して、利用法Uの第1のチケットT1をチケットサーバ装置2より入手し、次のようにして、利用法Uの第2のチケットT2を得る。

【0115】チケット鍵生成手段152により、前記第2のチケットT2を生成する際、まず乱数発生手段153で、乱数Rを得る(ステップA'4-1)。以下、当該乱数Rを、真のチケット鍵と呼ぶ。

【0116】そして、鍵分割手段654で、前記真のチケット鍵Rと、第1のチケットT1のチケット鍵K1を用いて、数式1により第2のチケットT2のチケット鍵K2を算出する(ステップA'4-2)。なお、当該手順を示した模式図を図19に示す。

【0117】

【数1】 $K2 = f(K1, R)$

【0118】ここで、関数fは、次の数式2と数式3とを同時に満たす。

【0119】

【数2】 $|f(a, b)| \sim |a| \sim |b|$

($|x|$ は正整数xのビット数を示し、 \sim は近似であることを示す)

【数3】 $f(b1, b2) = f(b2, b1)$

【0120】また、関数fは、 $a = f(b1, b2)$ のとき、次の数式4及び数式5となる逆関数f invが存在するような、関数である。

【数4】 $b2 = f\text{ inv}(b1, a) = f\text{ inv}(a, b1)$

【数5】 $b1 = f\text{ inv}(a, b2) = f\text{ inv}(b2, a)$

【0121】なお、関数fの具体例としては、数式6に示すものがある。

【数6】 $f(a, b) = a \text{ XOR } b$

(XORは排他的論理和)

この場合、 $f = f\text{ inv}$ である。

【0122】第2のチケット鍵生成後、前記利用法Uの利用秘密情報を生成する。前段で生成された暗号化著作物データの復号鍵Kを前記真のチケット鍵Rを用いて、暗号化手段151により暗号化し、当該利用法の利用秘密情報を得る(ステップA'4-3)。

【0123】以上のようにして生成された第2のチケット鍵は、第1の実施の形態と同様に、利用条件記述中に埋め込まれ(ステップA'5)、チケットサーバ装置2に登録される(ステップA'6)。

【0124】一方、前記利用秘密情報から第1の実施の形態と同様に、前記アクセス制御テーブルが生成される。さらに、前記第2のチケット鍵の他に、前記第1の

チケットが必要となることを示すよう、チケット発行元リストが生成される。当該アクセス制御テーブルと当該チケットリストなどの著作物情報と前記暗号化著作物データとを含めて連結され、図20に示すような構造をもつ第2のカプセル化著作物が生成され（ステップA'7）、流通センタ装置3に登録される（ステップA'8）。

【0125】次に、図16のステップC'の処理について、図17を参照して詳細に説明する。利用者は、利用法Uにより当該著作物を利用を要求する（ステップC'1）。そして、当該著作物の著作物情報から、前記チケットリストを参照し、必要となるチケットを判定する（ステップC'2）。

【0126】まず、チケットインターフェース部44で、前記第2のチケットをチケットサーバ装置2に要求する（ステップC'3）。

【0127】当該要求を受けたチケットサーバ装置2は、第1の実施の形態と同様に、第2の著作物についての利用条件記述に、当該要求が合致するかどうかを判定し、合致すれば、第2のチケット鍵を生成し、第2の視聴装置7に送信する（ステップC'4）。

【0128】次に、同様にして、第2の視聴装置7は、前記第1のチケットをチケットサーバ装置2に要求し（ステップC'5）、チケットサーバ装置2は、条件判定した上で当該チケットを送信する（ステップC'6）。

【0129】こうして受信した第1および第2のチケットは、視聴装置7のカプセル化解除部48で、前記カプセル化著作物より著作物データを復元するために、鍵結合手段782で、当該第1および第2のチケットから前記第1のチケット鍵K1および第2のチケット鍵K2を抽出し、数式7の計算を行う（ステップC'7）。

【数7】 $R' = \text{finv}(K1, K2)$

【0130】このとき、前記真のチケット鍵Rについて、数式8が成り立つ。

【数8】 $R' = R$

【0131】そして、復号手段481は、R'と前記利用秘密情報テーブル中の利用法Uに対応する利用秘密情報とを用いて、前記暗号化著作物データの復号鍵Kを復元する（ステップC'8）。

【0132】その後、復号手段481は、当該復号鍵Kと当該暗号化著作物データとを用いて、再び前記第2の著作物データを復元する（ステップC'9）。

【0133】本実施の形態では、二次的著作物の流通について、当該著作物に関する一次著作者および二次著作者の発行するチケットが同時に必要となるため、二次的著作物の著作権保護がより強固なものとなる。さらに、一般に巨大なサイズをもつ暗号化著作物データの復号処理は、この場合においても、1回のみであり、再生処理のスループット低下を最小限に抑えることができる。

【0134】[第3の実施の形態]図21を参照すると、編集装置8が、図1に示された第1の実施の形態における編集装置1の構成に加え、課金モジュール編集部87と、課金モジュール蓄積部88とを有する点で異なる。また、視聴装置9が、図1に示された第1の実施の形態における視聴装置4の構成に加え、課金処理部98と課金モジュール蓄積部99とを有する点で異なる。さらに、電子財布装置101および決済サーバ装置111が図1に示された第1の実施の形態の構成に加えられている点で異なる。

【0135】課金モジュール編集部87では、課金モジュールのソースコードを編集し、その実行形式を生成する。

【0136】課金モジュール蓄積部88では、前段で作成された課金モジュールの実行形式を蓄積する。

【0137】課金処理部98は、実行キュー管理手段981と、課金モジュール実行手段982とを備え、課金モジュール蓄積部99に蓄積された課金モジュールの実行を行う。

【0138】課金モジュール蓄積部99は、カプセル化著作物に同梱された課金モジュールを蓄積する。

【0139】電子財布装置101は、視聴装置9で発生した課金額を、決済予定金として記録し、定期的に決済サーバ装置111と決済処理のための通信を行う。

【0140】決済サーバ装置111は、電子財布装置101との通信により、決済情報を所定の金融機関に送信し、販売者または著作者への適切な振込処理を行う。

【0141】なお、図21の著作物流通システムにおいて、電子財布装置101と決済サーバ装置111とは、視聴装置9と同一のコンピュータ装置上に実現することも可能である。

【0142】以下、本実施の形態の動作について、説明する。

【0143】まず、本実施の形態の動作全体の概略について、図22を参照して説明する。著作者は、第1の実施の形態と同様に、著作物データの編集して登録し、また、利用条件を設定する。さらに、ここでは、課金方法と課金額も設定する（ステップA''）。

【0144】次に、利用者は、視聴装置9で、カプセル化著作物インターフェース部により、前記カプセル化著作物を取得する（ステップB'1）。取得後、カプセル化著作物インターフェース部46は、当該カプセル化著作物から課金モジュールを抽出し、課金モジュール蓄積部99に蓄積する。課金モジュールが除かれたカプセル化著作物は、カプセル化著作物蓄積部47に蓄積される（ステップB'2）。

【0145】利用者は、その著作物について利用要求を行い、当該著作物のチケットをチケットサーバ装置2から取得して視聴装置4に蓄積する。さらに、ここでは、カプセル化著作物に対する課金処理も実行する（ステッ

ブC'')。そして、再生処理部43は、第1の実施の形態と同様に、著作物データの再生処理を行い、利用者による利用を可能にする(ステップD)。

【0146】次に、図22のステップA''の処理について、図23を参照して詳細に説明する。著作者は、第1の実施の形態と同様に、編集装置8で、著作物データを作成する(ステップA''1)。次に、当該著作物データに対して利用条件設定部13で、各利用法ごとの利用条件を設定する。この際、第1の実施の形態における利用条件設定に加え、課金方法と課金額を設定するため、課金モジュール蓄積部88に蓄積された課金モジュールの中から適当なものを選択する。もし、適当な課金モジュールがなければ、課金モジュール編集部87で、新規な課金モジュールを作成し、使用することができる。そして、課金額や課金方法の詳細なパラメータなどを設定する。当該設定内容は、当該課金モジュールへの引数の形に変換される(ステップA''2)。

【0147】次に、カプセル化処理部15で、前記著作物データの暗号化が行われる(ステップA''3)。そして、前記のように各利用法ごとに設定された課金モジュールについて、それぞれの実行形式を含む、一つの課金モジュールアーカイブが生成される(ステップA''4)。そして、第1の実施の形態におけるカプセル化処理部15の動作と同様に、チケット鍵および利用秘密情報が生成され(ステップA''5)、前記暗号化著作物データと、利用秘密情報テーブルと、その他著作物情報と、前記課金モジュールアーカイブとから、図25に示したような構造をもつカプセル化著作物が生成され(ステップA''6)、流通センタ装置3に登録される(ステップA''7)。

【0148】一方、前記課金モジュールの名前とその引数は、前記チケット鍵と同様に、利用条件記述中に埋め込まれ(ステップA''8)、登録インターフェース部16を介して、チケットサーバ装置2に登録される(ステップA''9)。

【0149】次に、図22のステップC''の処理について、図24を参照して詳細に説明する。当該カプセル化著作物の利用が行われる際、まず必要となるチケットが既に取得済みであるかどうかを判定し(ステップC''1)、未取得であった場合、第1の実施の形態における視聴装置4と同様にして、チケットサーバ装置2よりチケットを取得し、蓄積する(ステップC''2〜C''7)。既に当該チケットが取得済みであった場合、蓄積されたチケットにより、著作物データの復元処理へ進む。

【0150】ここで、当該チケットには、第1の実施の形態におけるチケットの記述(著作物IDや著作者IDなど)に加えて、前記課金モジュール名と、課金額などの当該課金モジュールへの引数に関する記述が、課金情報として、課金情報フィールドの中に含まれている(図

26)。

【0151】さらに、視聴装置9は、カプセル化解除部48で、前記チケットを用いて、カプセル化著作物を、第1の実施の形態における視聴装置4と同様にして、当該カプセル化著作物に含まれるデータを分割する(ステップC''8)。

【0152】その後、視聴装置9、チケット中の課金情報フィールドを参照し、その内容を課金処理部98に伝える。課金処理部98では、当該課金情報を、実行キュー管理手段981に記録する(ステップC''9)。実行キュー管理手段では、図27に示されるように、チケットシリアル番号と、課金モジュール名と、課金額やその他の当該課金モジュールへの引数とが、テーブルの形で保持される。以下、このテーブルを実行キューと呼ぶ。

【0153】次に、課金処理部98は、前記実行キューに登録された当該チケットに対応する課金モジュールを、課金モジュール蓄積部99より抽出し、課金モジュール実行手段982で実行し、課金処理を行う(ステップC''10)。

【0154】課金モジュールは、課金方法を記述したプログラムであり、利用時に指定の課金額を収め、繰り返し同じ利用法による利用が可能となる一括方式や、回数に関わらず利用時に一定の課金額を収める必要のあるペイ・パー・ビュー方式などといった課金方法を記述できる。視聴装置9で、プログラムの内容に関わらず、一定の呼び出し規約により、課金処理を行うことができるように、図28に示したような基本メソッドが、著作者もしくは販売者により定義されていることが規定されている。また、視聴装置9が有する各部を駆動するための手続きが、組込メソッドとして予め定義されており、課金モジュール内部で当該組込メソッドを呼び出すことにより、電子財布装置101へ課金情報を渡すなどといった処理を行うことができる。また、その他著作者に任意により定義されたユーザ定義メソッドも使用できる。基本メソッドの定義では、これら組込メソッドとユーザ定義メソッドを、適当に組み合わせて呼び出すことにより、様々な課金処理を行うことができる(図29)。

【0155】課金モジュールによる具体的な課金処理の例を示す。まず、課金モジュールは、charge()という基本メソッドを必ず備えており、課金モジュール実行手段982はモジュールの種類によらずcharge()メソッドに、前記基本メソッドの引数(課金額および対応チケット、その他の情報)とともに、呼び出すことにより、課金処理を実行できるようにプログラムされている。そして、charge()メソッドが呼ばれると、引数として受け取った課金額とその振込先に関する情報を電子財布装置101に伝える。電子財布装置101では、前記課金額情報を保持し、一定時間間隔(例えば1日)で、決済サーバ装置111と通信して、決済

処理を行う。決済サーバ装置10では、前記振込先に対して前記課金額を振り込むための処理を行う。

【0156】また、必要に応じて、もう一つの基本メソッドである`expire()`が呼び出される。`expire()`メソッドの実行により、前記実行キューからの当該課金モジュールの削除が行われる。さらに、`disable_ticket()`が呼び出されると、前記対応チケットの無効化が行われる。無効化されたチケットは、それ以降の著作物の利用時に、視聴装置9で通常のチケットとして扱われることはない。また、`transmitToWallet()`が呼び出されると、引数に示された額が決済予定金として、電子財布装置9に記録される。

【0157】課金モジュールの具体的な構成例としては、最初の`charge()`メソッド呼出して、`expire()`メソッドと`disable_ticket()`メソッドが呼び出されると、いわゆるペイ・パー・ビュー方式の課金が実現できる。また、最初の`charge()`メソッド呼出して、`expire()`メソッドのみが呼び出された場合、従来の購入方式（商品の受取時に対価を支払う）が実現される。さらに、購入日時と利用可能期間を`charge()`メソッドへの引数として呼び出し、当該購入日時から当該利用可能期間を経た日時に`expire()`メソッドおよび`disable_ticket()`メソッドが呼び出された場合、ビデオレンタルなどのような時限付課金方式が実現できる。

【0158】本実施の形態では、適切な課金モジュールの適用により、著作者や販売者の意向と、著作物の性格などにより、効果的な課金方法の選択が柔軟にできるようになる。さらに、課金処理と決済処理を2段階に分けて行い、電子財布装置100と決済サーバ装置101との間の通信にはSETなど従来の電子決済方式が適用できるため、既存の決済機構との親和性にも優れている。

【0159】〔実施の形態の変形〕本発明は、上記の実施の形態に限られず、種々の変形、応用が可能である。以下、本発明に適用可能な上記の実施の形態の変形態様について、説明する。

【0160】上記の第1の実施の形態において、編集装置1で生成したカプセル化著作物を、登録インターフェース部16を介して流通センタ装置3へ登録することなく、書き込み可能なコンパクトディスクなどの不揮発性メモリにカプセル化著作物を書き出してもよい。この選択は、著作者の任意による。そして、視聴装置4でカプセル化著作物を取得する場合、流通センタ装置3にアクセスするのではなく、上記不揮発性メモリを取得し、カプセル化著作物蓄積部44で当該不揮発性メモリをアクセスできるようにする。この場合は、当該不揮発性メモリを店舗に置くなどの物理世界での流通が可能となり、著作物データのサイズが非常に大きくなり、ネットワー

ク上を流通させることが困難な場合にも対応できる。

【0161】上記の第2の実施の形態において、鍵分割手段654は、鍵分割関数として、前記真のチケット鍵Rを鍵とする共有鍵暗号を用いて一次著作者のチケット鍵K1から二次著作者のチケット鍵K2を生成することもできる。この場合、鍵統合手段782では、チケット鍵K2を鍵として前記共有鍵暗号によりK1からRを復元する。もっとも、第n次著作物（ $n > 2$ ）のチケット鍵生成には、前記のように共有鍵暗号をもちいた鍵分割を行うことはできない。

【0162】その点、前記鍵分割関数fを用いることで、このような第三次以降の著作物のチケット鍵生成が可能になる。この場合、n次著作者は、第一次～第（ $n-1$ ）次著作者のチケット鍵K1～K $n-1$ を取得し、真のチケット鍵Rを乱数により生成し、鍵分割手段654で、前記鍵分割関数fに対して、数式9を計算する。

【数9】 $K_n = f(K_1, K_2, \dots, K_{n-1}, R)$

【0163】また、鍵統合手段782では、前記と同様に、次の数式10を計算して、真のチケット鍵Rを復元する。

【数10】 $R = f_{inv}(K_1, K_2, \dots, K_{n-1}, K_n)$

こうした場合、第（ $n-1$ ）次著作者までのチケット鍵K1～K $n-1$ の取得順序は任意でよい。

【0164】上記の第1～第3の実施の形態では、チケット鍵には、暗号と復号とで共通の鍵を使用する対称鍵暗号系を用いていた。これに対し、チケット鍵には、暗号と復号とで別の鍵が用いられる非対称鍵暗号系を用いてもよい。

【0165】上記の第1～第3の実施の形態では、編集装置1、6、8と、チケットサーバ装置2と、流通センタ装置3とは、それぞれ別個のコンピュータ装置上で実現され、ネットワークで接続されるものとしていた。しかしながら、これらのすべて或いはそのうちの任意の2つを、同一のコンピュータ装置上で実現することも可能である。

【0166】上記の第1～第3の実施の形態では、編集装置1、6、8、チケットサーバ装置2、流通センタ装置3、（第1、第2を含む）視聴装置4、5、7、9には、それぞれ各部、手段の機能が実現されているものとしていた。これに対し、これらの機能を実現するためのプログラムは、CD-ROMやフロッピーディスクなどのコンピュータ読み取り可能な記録媒体に格納して配布してもよい。

【0167】

【発明の効果】以上説明したように、本発明によれば、配信されるカプセル化著作物にはその著作物データの復号鍵が含まれていないため、著作物データを自由に配布することが可能となる。そして、著作物データを利用さ

せる場合には、チケット配信手段からチケット復号鍵を配信するだけでよく、著作物の流通範囲の拡大と利用促進を望めるようになる。

【0168】また、著作物データの利用条件毎に異なるチケット鍵（暗号鍵及び復号鍵）が生成することができる。このため、著作者及び販売者の意図を反映させて、利用条件を設定し、著作物データを利用させることができる。

【0169】さらに、二次著作物データを生成し、生成された二次著作物データを配布すべき著作物データとすることで、一次著作物データと同様に流通させることができるので、著作活動の活性化が可能となる。また、その基となる著作物データのチケット復号鍵も必要となるので、一次著作者の権利保護を十分に図ることができる。

【0170】さらに、課金モジュールを利用条件毎に生成し、課金処理を課金モジュールで行うことにより、著作者や販売者の意図、或いは著作物の性格などに従って、適切な課金方法を柔軟に選択することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態の著作物流通システムの構成を示すブロック図である。

【図2】本発明の第1の実施の形態の動作の概略を示す流れ図である。

【図3】本発明の第1の実施の形態における編集装置の動作を示す流れ図である。

【図4】本発明の第1の実施の形態における流通センタ装置と視聴装置との通信動作を示す流れ図である。

【図5】本発明の第1の実施の形態におけるチケットサーバ装置と視聴装置との通信動作を示す流れ図である。

【図6】利用条件設定ダイアログの一例である。

【図7】利用条件設定操作の一例である。

【図8】チケット鍵生成動作を示す図である。

【図9】利用秘密情報テーブルの一例である。

【図10】本発明の第1の実施の形態におけるカプセル化著作物の構造の一例である。

【図11】利用条件記述の構造と、アクセス制御言語による利用条件記述の一例である。

【図12】著作物が複数オブジェクトから構成される場合の階層構造の一例と、そのアクセス制御言語による利用条件記述の一例である。

【図13】流通センタ装置にアクセスした際、視聴装置で表示される著作物インデックス画面の一例である。

【図14】本発明の第1の実施の形態におけるチケットの構造の一例である。

【図15】本発明の第2の実施の形態の著作物流通システム構成を示すブロック図である。

【図16】本発明の第2の実施の形態の動作の概略を示す流れ図である。

【図17】本発明の第2の実施の形態における第1の視

聴装置および編集装置の動作を示す流れ図である。

【図18】本発明の第2の実施の形態におけるチケットサーバ装置と第2の視聴装置との通信動作を示す流れ図である。

【図19】分割関数を用いた第2のチケット鍵生成を示す図である。

【図20】本発明の第2の実施の形態におけるカプセル化著作物の構造の一例である。

【図21】本発明の第3の実施の形態の著作物流通システムの構成を示すブロック図である。

【図22】本発明の第3の実施の形態の動作の概略を示す流れ図である。

【図23】本発明の第3の実施の形態における編集装置における動作を示す流れ図である。

【図24】本発明の第3の実施の形態におけるチケットサーバ装置と視聴装置との通信動作を示す流れ図である。

【図25】本発明の第3の実施の形態におけるカプセル化著作物の構造の一例である。

【図26】本発明の第3の実施の形態におけるチケットの構造の一例である。

【図27】実行キューの一例である。

【図28】課金モジュールにおけるメソッド種別と、各メソッドの機能の一例である。

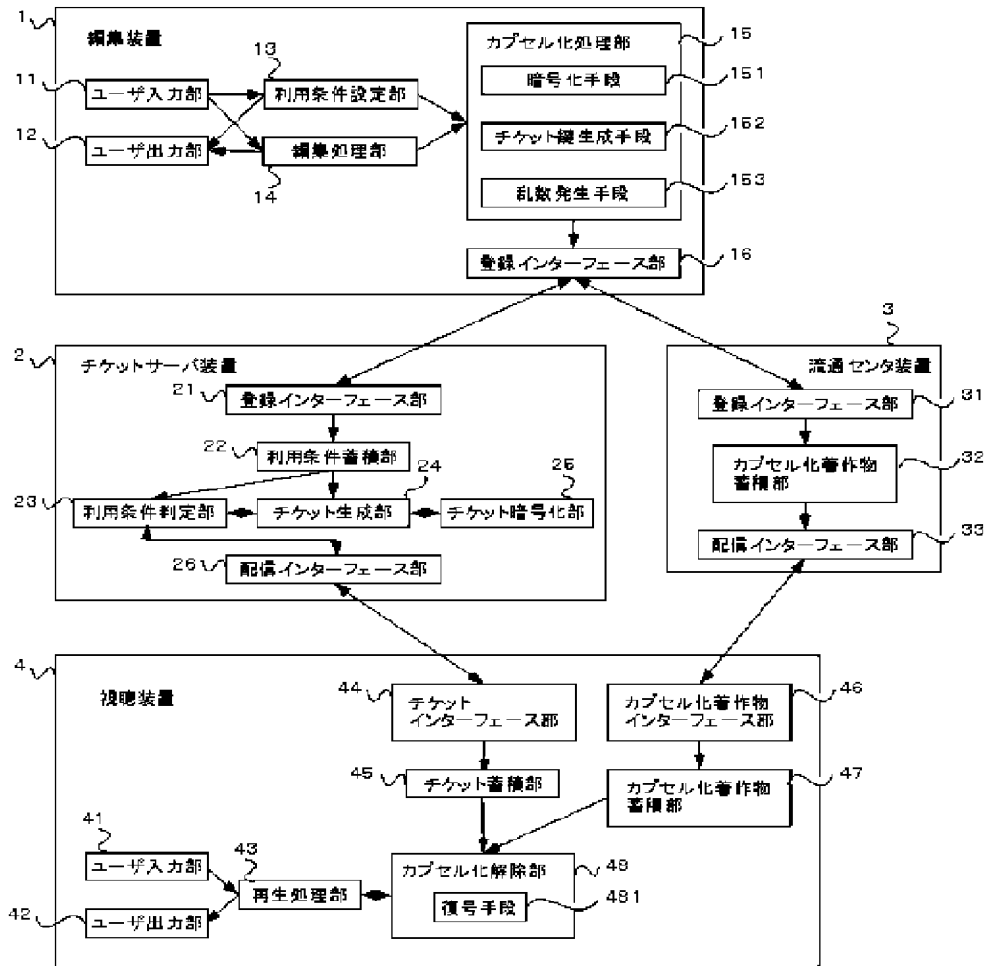
【図29】課金モジュールの構造と、その具体例を示す図である。

【符号の説明】

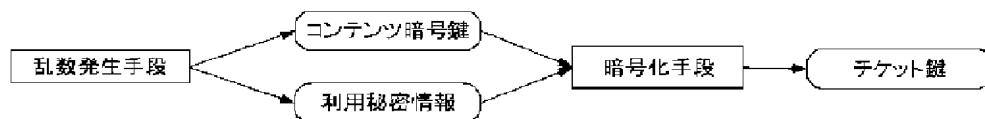
- | | |
|-----|-------------|
| 1 | 編集装置 |
| 11 | ユーザ入力部 |
| 12 | ユーザ出力部 |
| 13 | 利用条件設定部 |
| 14 | 編集処理部 |
| 15 | カプセル化処理部 |
| 151 | 暗号化手段 |
| 152 | チケット鍵生成手段 |
| 153 | 乱数発生手段 |
| 16 | 登録インターフェース部 |
| 2 | チケットサーバ装置 |
| 21 | 登録インターフェース部 |
| 22 | 利用条件蓄積部 |
| 23 | 利用条件判定部 |
| 24 | チケット生成部 |
| 25 | チケット暗号化部 |
| 26 | 配信インターフェース部 |
| 3 | 流通センタ装置 |
| 31 | 登録インターフェース部 |
| 32 | カプセル化著作物蓄積部 |
| 32 | 配信インターフェース部 |
| 4 | 視聴装置 |
| 41 | ユーザ入力部 |

- | | | | |
|-----|-------------------|-----|-------------|
| 42 | ユーザ出力部 | 782 | 鍵統合手段 |
| 43 | 再生処理部 | 8 | 編集装置 |
| 44 | チケットインターフェース部 | 87 | 課金モジュール編集部 |
| 45 | チケット蓄積部 | 88 | 課金モジュール蓄積部 |
| 46 | カプセル化著作物インターフェース部 | 9 | 視聴装置 |
| 47 | カプセル化著作物蓄積部 | 98 | 課金処理部 |
| 48 | カプセル化解除部 | 981 | 実行キュー管理手段 |
| 481 | 復号手段 | 982 | 課金モジュール実行手段 |
| 5 | 視聴装置 | 99 | 課金モジュール蓄積部 |
| 6 | 編集装置 | 101 | 電子財布装置 |
| 653 | 鍵分割手段 | 111 | 決済サーバ装置 |
| 7 | 視聴装置 | | |

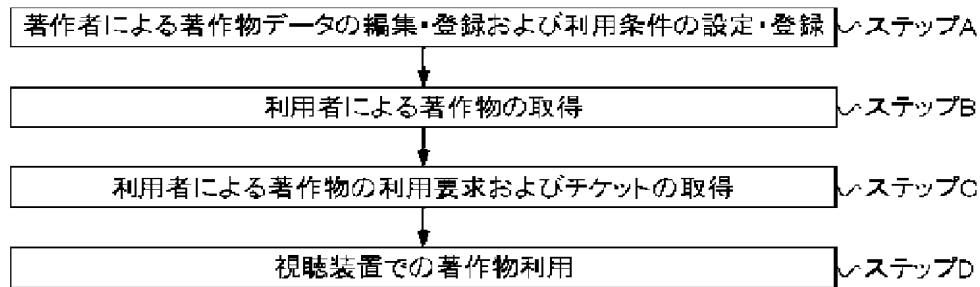
【図1】



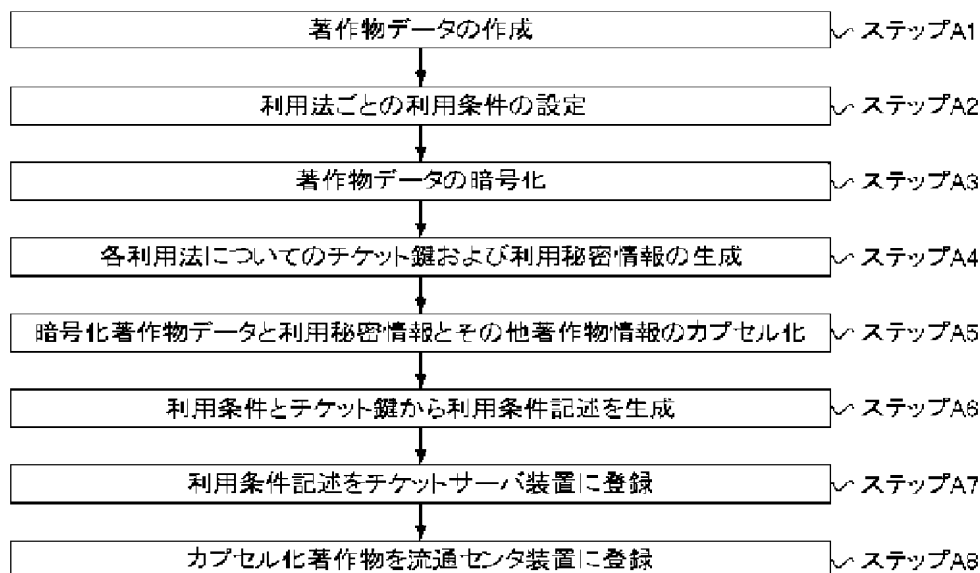
【図8】



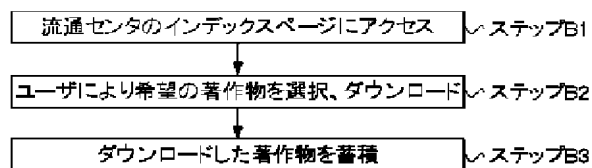
【図2】



【図3】



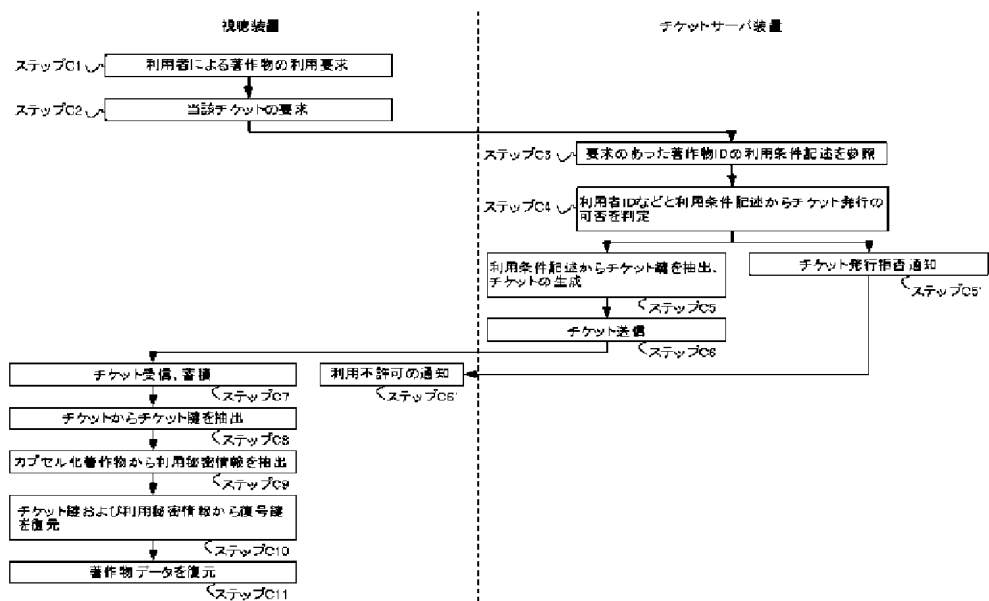
【図4】



【図6】

利用条件設定ダイアログ			
著作者ID:	Nakae		
著作物ID:	Movie980506		
制御対象			
閲覧:	<input checked="" type="radio"/> いつでも許可	<input type="radio"/> 条件を設定	<input type="radio"/> 許可しない
保存:	<input type="radio"/> いつでも許可	<input type="radio"/> 条件を設定	<input checked="" type="radio"/> 許可しない
印刷:	<input type="radio"/> いつでも許可	<input checked="" type="radio"/> 条件を設定	<input type="radio"/> 許可しない
編集:	<input type="radio"/> いつでも許可	<input type="radio"/> 条件を設定	<input checked="" type="radio"/> 許可しない
OK		キャンセル	

【 図 5 】



【 図 7 】

利用条件設定ダイアログ

著作権ID:

著作物ID:

利用対象

閲覧:	<input checked="" type="radio"/> いつでも許可	<input type="radio"/> 条件を設定	<input type="radio"/> 許可しない
保存:	<input type="radio"/> いつでも許可	<input type="radio"/> 条件を設定	<input checked="" type="radio"/> 許可しない
印刷:	<input type="radio"/> いつでも許可	<input checked="" type="radio"/> 条件を設定	<input type="radio"/> 許可しない
編集:	<input type="radio"/> いつでも許可	<input type="radio"/> 条件を設定	<input checked="" type="radio"/> 許可しない

印刷の条件設定

許可対象者リスト:

制限事項

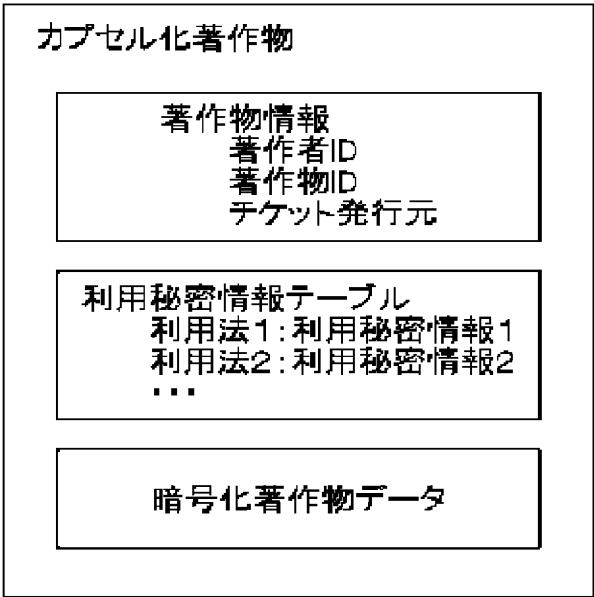
カラー:	<input type="text" value="256"/> 色以下
品質:	<input type="text" value="600"/> dpi以下
用紙:	<input type="text" value="A4"/> 以下

課金額: 円

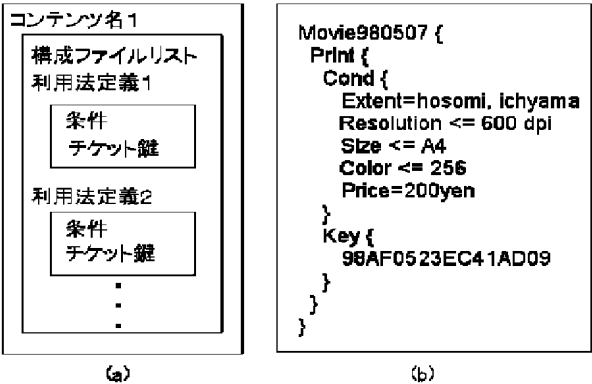
【 図 9 】

利用法	秘密情報
閲覧	95AD438A
保存	N/A
印刷	F38F05AD
編集	N/A

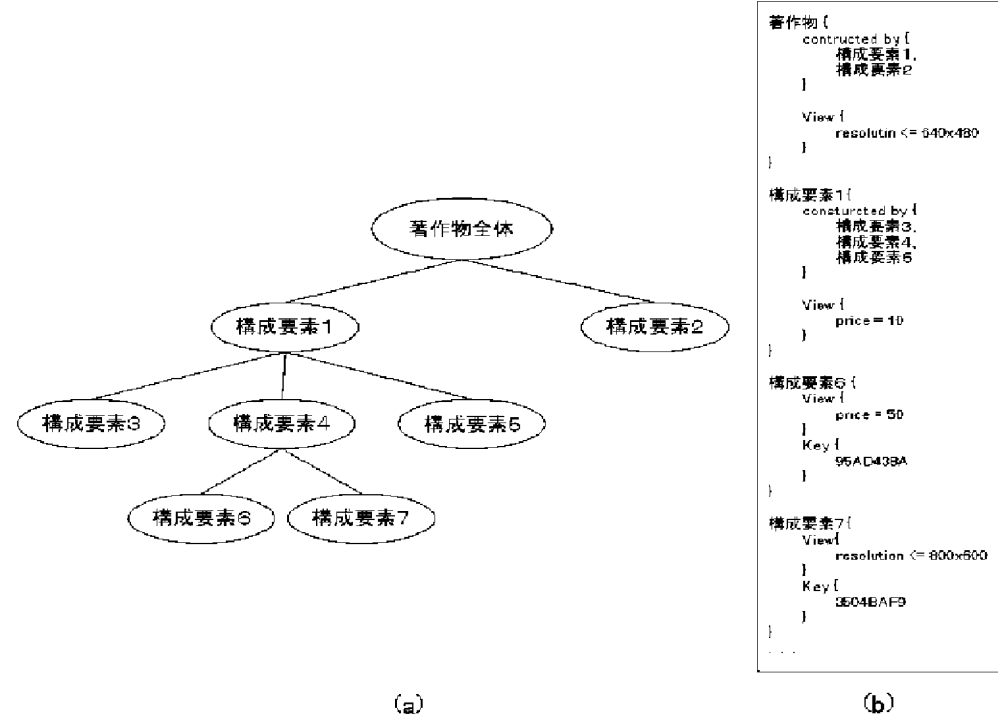
【図10】



【図11】



【図12】



著作物 {
constructed by {
構成要素1,
構成要素2
}

View {
resolution <= 940x480
}
}

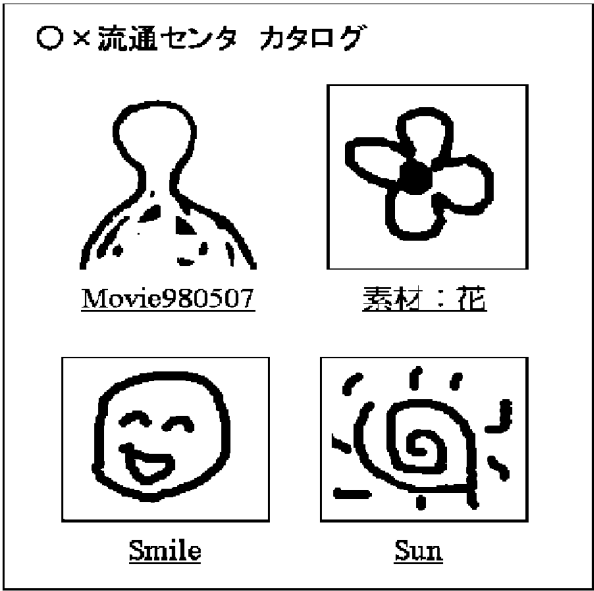
構成要素1 {
constructed by {
構成要素3,
構成要素4,
構成要素5
}

View {
price = 10
}
}

構成要素3 {
View {
price = 50
}
Key {
95AD439A
}
}

構成要素7 {
View {
resolution <= 800x600
}
Key {
3E04BAF9
}
}
...
}

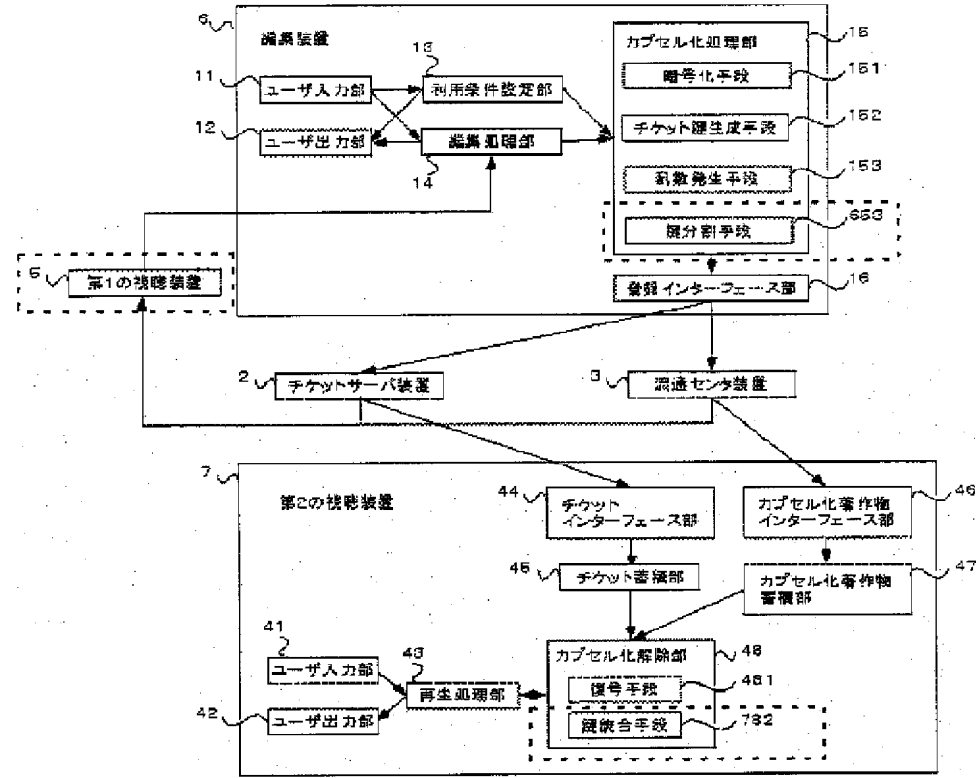
【図13】



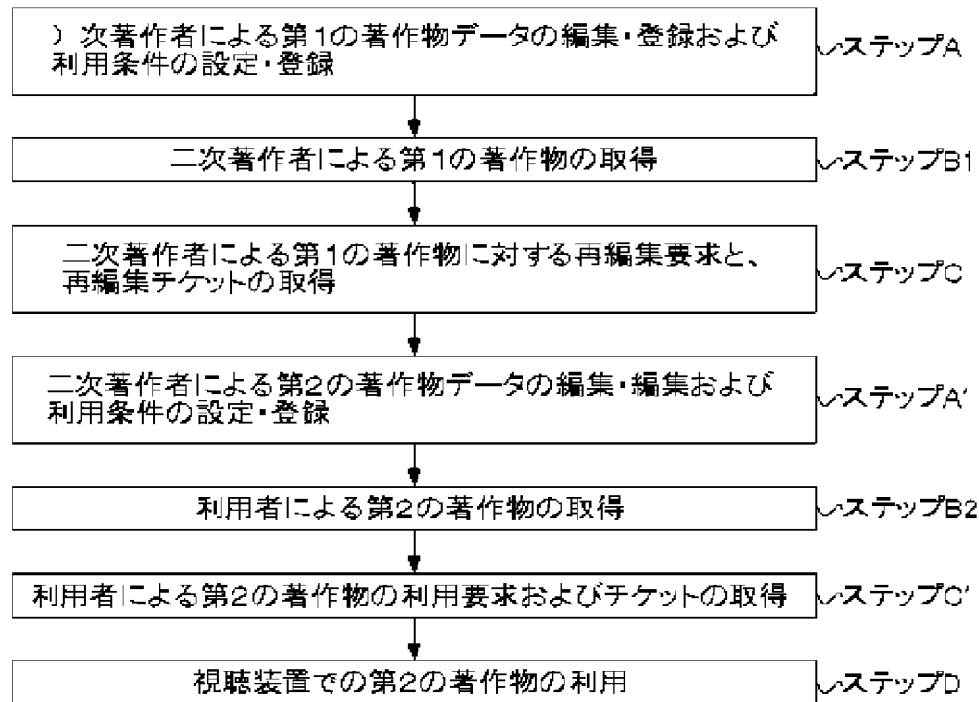
【図14】

著作物ID	Movie980507
利用者ID	nakae
チケットシリアル番号	TK980507.AZK8311
チケット鍵	98AF0523EC41AD09
許可された利用法	Print
発行年月日	1998/05/07
有効期限	1999/05/07

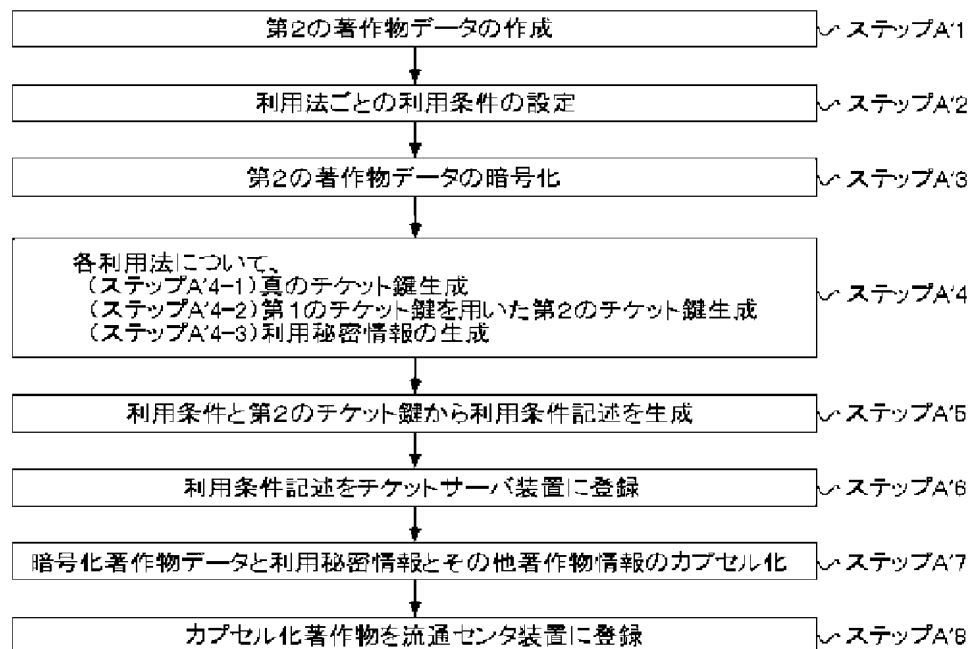
【図15】



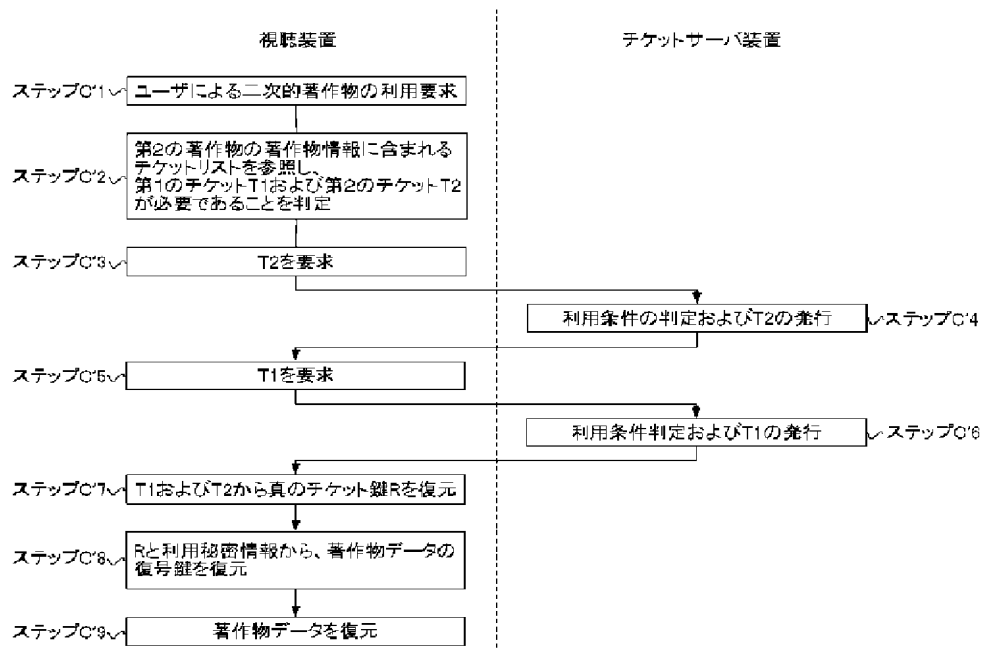
【図16】



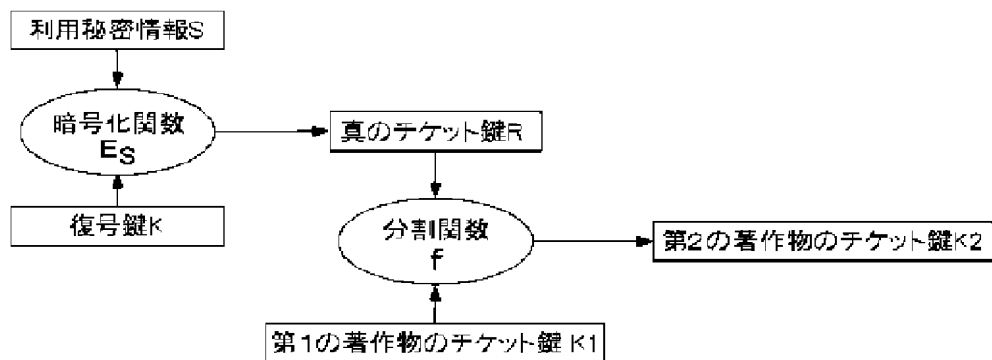
【図17】



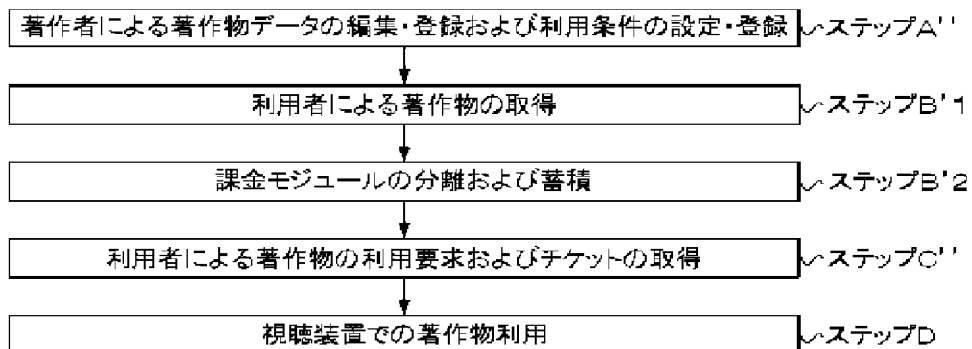
【図18】



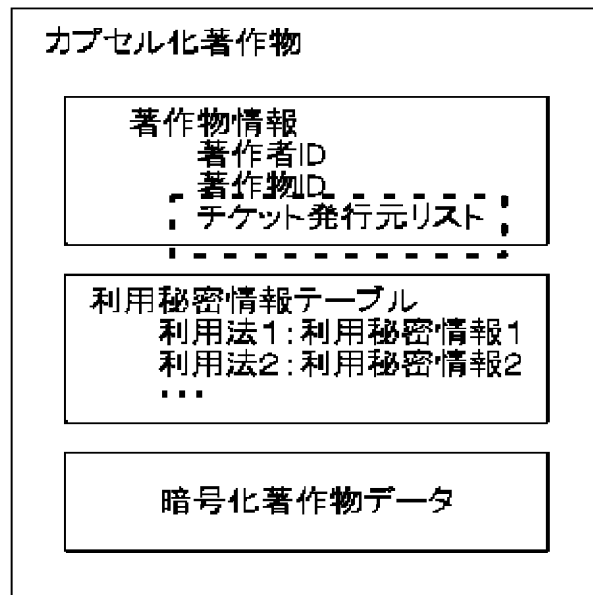
【図19】



【図22】



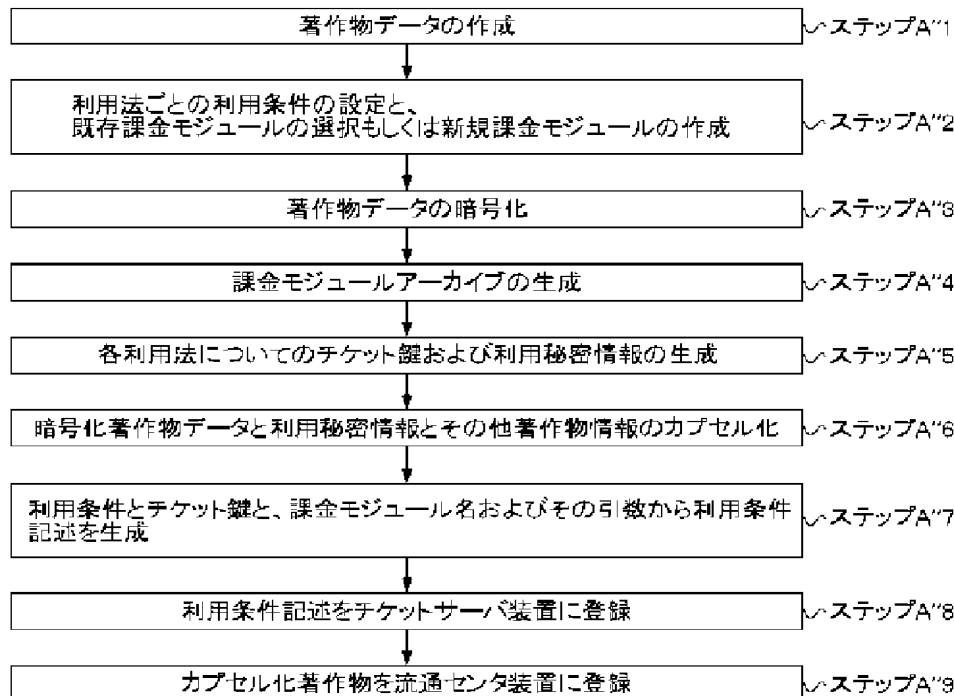
【図20】



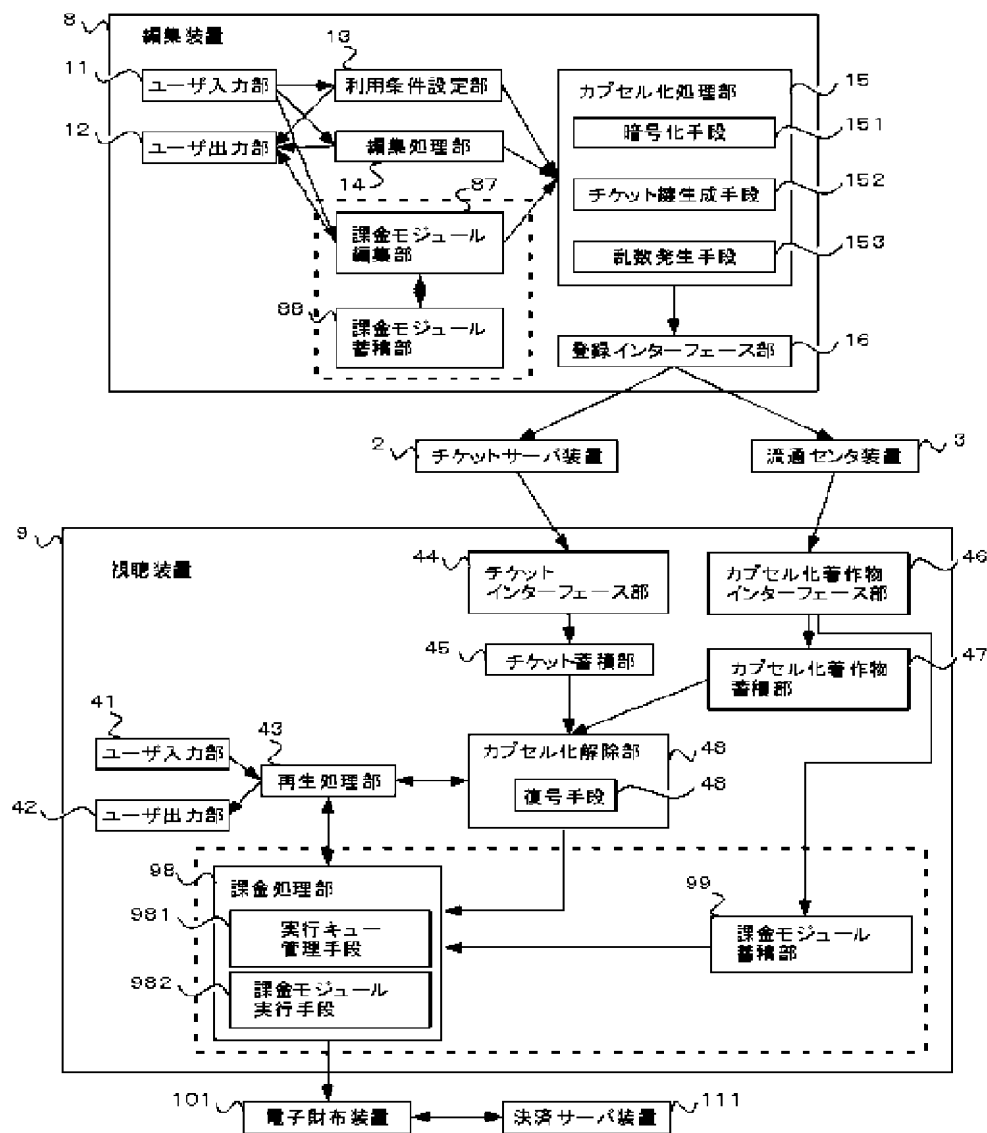
【図26】

著作物ID	Movie980507
利用者ID	nakae
チケットシリアル番号	TK980507.AZK8311
チケット鍵	98AF0523EC41AD09
許可された利用法	Print
課金モジュール名	chargeAtOnce
課金モジュールへの引数	4,000yen
発行年月日	1998/05/07
有効期限	1999/05/07

【図23】



【図21】

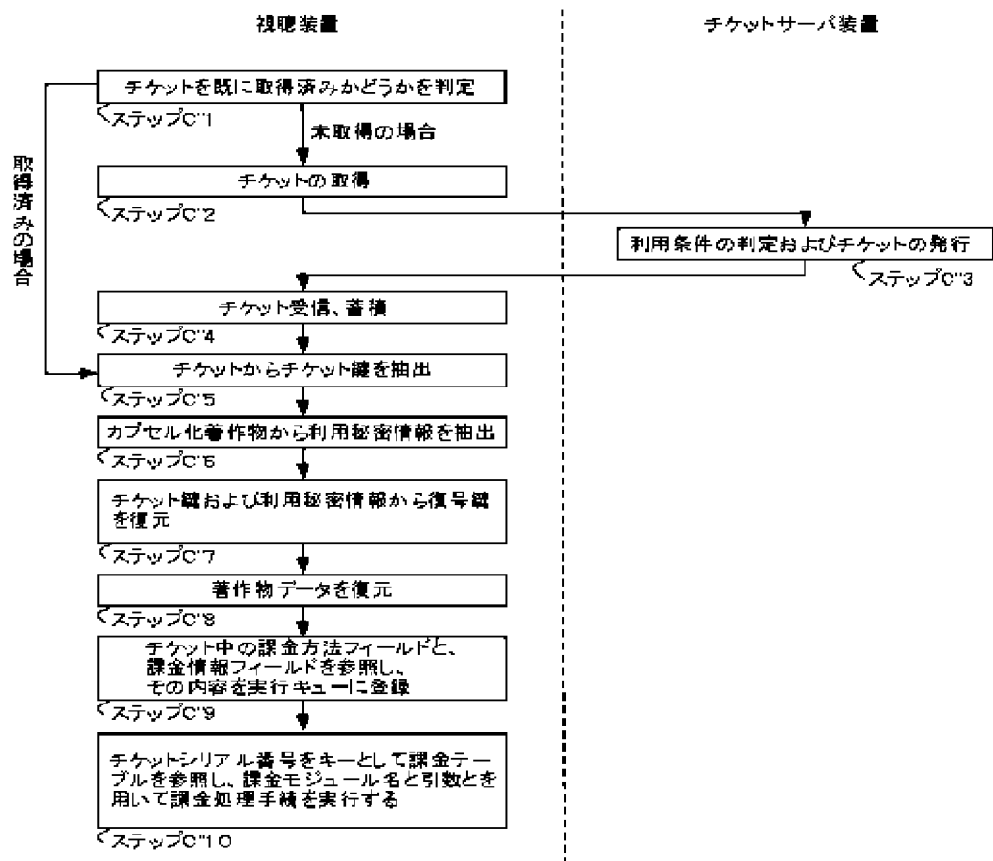


【図27】

実行キュー

チケットシリアル番号	モジュール名	引数	モジュール呼出
TK980507.AZK8311	chargeAtOnce	4,000yen	chargeAtOnce("4000yen")
TK970120.FA15001	chargePerUse	50yen	chargePerUse("50yen")
TK980507.GEDA99	chargeTill	500yen, 12:00 Aug 18 1998	chargeTill("500yen", "12:00 Aug 18 1998")
...	

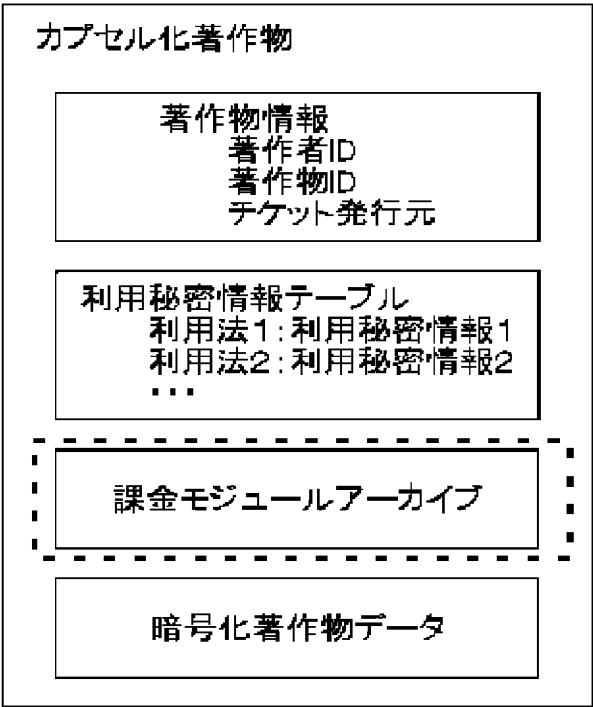
【図24】



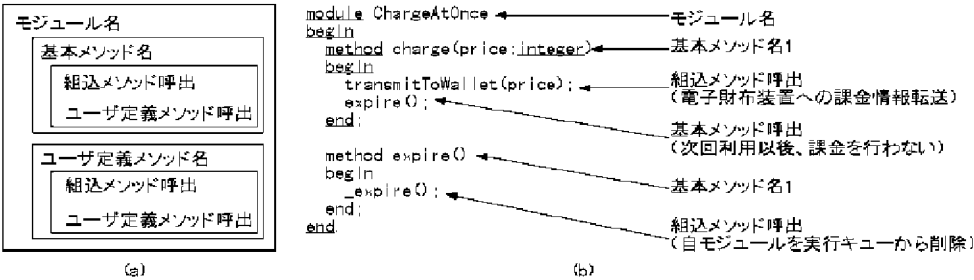
【図28】

基本メソッド	change()	課金処理を行う
	expire()	自課金モジュールを実行キューから削除し、それに伴う処理を行う
組み込みメソッド	disableTicket()	チケットの無効化を行う
	transmitToWallet()	課金情報を電子財布装置に渡す
	timer()	定期的にchange()を呼ぶよう設定を行う
	expire()	実際に自課金モジュールを実行キューから削除
ユーザ定義メソッド	著作者により自由に定義	

【図25】



【図29】



フロントページの続き

(51)Int.Cl. ⁷	識別記号	F I	テマコード ⁷ (参考)
H 0 4 L	9/08	H 0 4 L	9/00
	9/32		6 0 1 C
			6 0 1 Z
			6 7 5 A